JULIANA CHAVES MELILO

SISTEMAS DE SEGURANÇA RELACIONADOS AO ACESSO À INTRANET: O CASO DO TRT

FLORIANÓPOLIS, 2005

JULIANA CHAVES MELILO

SISTEMAS DE SEGURANÇA RELACIONADOS AO ACESSO À INTRANET: O CASO DO TRT

Trabalho de conclusão de estágio apresentado à disciplina Estágio Supervisionado – CAD 5236, como requisito parcial para obtenção do grau de Bacharel em Administração da Universidade Federal de Santa Catarina, área de concentração em informática.

Professora Orientadora:
Alessandra de Linhares Jacobsen

FLORIANÓPOLIS, 2005

JULIANA CHAVES MELILO

SISTEMAS DE SEGURANÇA RELACIONADOS AO ACESSO À INTRANET: O CASO DO TRT

Este trabalho de Conclusão de Estágio foi julgado adequado e aprovado em sua forma final pela Coordenadoria de Estágios do Departamento de Ciências da Administração da Universidade Federal de Santa Catarina, em _____/_____/_____.

Prof. Mário de Souza Almeida
Coordenador de Estágios

Apresentada à Banca Examinadora integrada pelos professores:

Alessandra de Linhares Jacobsen

Mário de Souza Almeida
Membro

Felipe Zurita Quadros
Membro

FLORIANÓPOLIS, 2005

Agradeço a minha família, meu pai Domingos Melilo, minha mãe, Jandira Chaves Melilo e meus irmãos, Jáder, Elaine e Luciana, pelo apoio, agradeço pela dedicação e atenção; a minha orientadora, profª Alessandra Jacobsen, que colaborou intensamente pela efetivação deste trabalho; e aos colaboradores do TRT: George A.Silva e Sandro Beltrame, por concederem a entrevista, permitindo que o estudo fosse realizado.

"Só é útil o conhecimento que nos torna melhores"

Sócrates

RESUMO

MELILO, Juliana Chaves. **Sistemas de segurança relacionados ao acesso à intranet – o caso do TRT/SC**. Número de folhas (106 folhas). Trabalho de Conclusão de Estágio (Graduação em Administração). Curso de Administração, Universidade Federal de Santa Catarina, Florianópolis.

Este trabalho foi desenvolvido visando analisar o uso de sistemas de segurança relacionados ao acesso á intranet, para tanto foi desenvolvido um estudo de caso no Tribunal Regional do Trabalho de Santa Catarina – Florianópolis. Buscou-se conciliar a teoria com a prática através da realização de entrevistas semi-estruturadas realizadas com George Alexandre Silva – Assistente-Chefe do Setor de Administração e Sistemas Operacionais e Sandro Beltrame – Diretor da Área de Suporte aos Recursos de Informática. Os dados foram obtidos por meio de perguntas abertas, através dos quais os entrevistados relacionaram os principais sistemas de segurança presentes na rede intranet. No entanto, o que se pôde constatar é que o TRT apresenta importantes mecanismos para conscientização da segurança entre seus usuários estando a organização atenta às formas de combater ataques e invasões de seus sistemas de rede.

Palavras- chaves: Intranet, Internet, Sistemas de Segurança, Redes.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

As organizações estão passando por profundas transformações em suas diversas áreas. A variedade de informações ao seu alcance contribui para o desenvolvimento de estratégias gerenciais interferindo em mudanças organizacionais. A disponibilidade de informações é tão importante para as empresas quanto a maneira pela qual devem dispor de sistemas seguros para mantê-las.

No entanto, por maiores que sejam os investimentos que se venham a realizar visando a melhoria dos sistemas de controle interno e de aspectos de segurança física e de dados, não se pode afirmar que exista sistema seguro, isento de erros, fraudes ou danos. Estes, quase nunca são provocados por equipamentos ou tecnologias, mas sim, pela ação do ser humano que muitas vezes, compõe a relação da equipe organizacional.

Algumas violações nos sistemas podem ser relativas à disseminação de vírus, erros intencionais, além de fraudes que ameaçam a integridade das informações da empresa. Ou seja, há várias possibilidades nesse sentido. Assim, dada a relevância das informações, bem como, a segurança destas, será feita uma análise quanto à segurança dos sistemas que controlam o acesso de usuários na Intranet, observando-os ainda como recursos de inovação tecnológica e mudança organizacional.

A rede (Intranet) considerada como base de estudo para a presente pesquisa diz respeito àquela que compõe a estrutura de transferência e comunicação de dados do TRT (Tribunal Regional do Trabalho), Empresa Pública, com sede em Florianópolis.

O Tribunal Regional do Trabalho da 12ª Região (anexo A) está localizado na rua Esteves Júnior, 377 - 1° andar – Centro. É um órgão pertencente à Justiça do Trabalho. Trata-se de um ramo do Poder Judiciário que tem por finalidade dirimir as questões decorrentes da relação de emprego, cuja competência é estabelecida na Constituição Federal.

Nesse sentido, compete à Justiça do Trabalho conciliar e julgar os dissídios individuais e coletivos entre trabalhadores e empregadores, abrangidos os entes de direito público externo e da administração pública direta e indireta dos Municípios, do Distrito

Federal, dos Estados e da União, e, na forma da lei, outras controvérsias decorrentes da relação de trabalho, bem como os litígios que tenham origem no cumprimento de suas próprias sentenças, inclusive coletivas (TRIBUNAL, 2005). O Tribunal Regional do Trabalho tem, por sua vez, competência para decidir sobre as questões trabalhistas ocorridas no âmbito do Estado.

As decisões proferidas pelo TRT, dependendo do tipo de processo que lhe é submetido, são em primeira instância (nas Varas ou Tribunal) ou segunda instância (processos de competência originária do Tribunal).

Nas localidades onde não existem Varas do Trabalho, e que não estejam sobre jurisdição destas, os Juízes de Direito estão encarregados legalmente de conhecer e julgar as questões que envolvam as relações de emprego (art. 668 da CLT).

Dentre as competências do Tribunal, além da matéria expressamente prevista em lei (TRIBUNAL, 2005), destacam-se:

a) Processar e julgar, em última instância, os pedidos de reconsideração das penas de natureza administrativa por ele próprio impostas.

b) Julgar:

- as argüições de inconstitucionalidade em processos de sua competência originária e as que lhe forem submetidas pelas Seções Especializadas ou pelas Turmas;

- as uniformizações de jurisprudência em processos que lhe forem submetidas pelas Seções Especializadas ou pelas Turmas;

- os mandados de segurança e os agravos regimentais contra atos do Presidente, do Vice-Presidente, do Corregedor e do próprio Tribunal;

- os embargos de declaração opostos a seus acórdãos;

- os incidentes e as ações incidentais de qualquer natureza, em processos sujeitos a seu julgamento;

- os conflitos de competência;

- as exceções de suspeição e de impedimento de seus membros;

- os incidentes de falsidade;

- julgar os recursos que lhe forem submetidos pelo Relator, sempre que reconhecer o

interesse público na assunção de competência.

c) Decidir sobre pedido de homologação de acordo celebrado em Juízo e de desistência requerida após a publicação da pauta e até o julgamento do feito, em processos submetidos a seu julgamento.

Em virtude de ser um órgão importante ao Estado, despertou-se interesse no sentido de analisar e estudar como funciona seu sistema de segurança especialmente no que tange aos potenciais riscos e ameaças existentes ao acesso da sua intranet, tendo em vista a dificuldade em manter um sistema 100% seguro diante de fraudes, violações e interferências de usuários mal-intencionados. Dessa forma, define-se como tema-problema da presente pesquisa o que segue:

1.1 Definição do tema – problema

Como sistemas de segurança relacionados ao acesso à intranet do TRT, órgão do setor público, são utilizados por seus usuários?

1.2 Objetivos

Em seguida são apresentados os objetivos geral e específicos projetados para a presente pesquisa.

1.2.1 Objetivo geral

Analisar o uso de sistemas de segurança relacionados ao acesso à intranet do TRT, sendo este um órgão público.

1.2.2 Objetivos específicos

a) Apontar o conteúdo e analisar o uso da intranet pelos usuários do TRT;
b) Identificar os sistemas de segurança relacionados à intranet do TRT;
c) Verificar as políticas de segurança em informática adotadas;
d) Levantar os mecanismos utilizados pelo TRT para reduzir o nível de resistência e conscientizar seus usuários quanto à segurança.

1.3 Justificativa

A elaboração desse estudo permite conhecer os fundamentos teóricos e conciliá-los com a prática organizacional. O TRT é uma empresa muito respeitada em Santa Catarina e também nacionalmente. Portanto, é interessante estudar como funciona seu sistema de informação, no que tange à sua rede digital de informações. Considerando-se ainda a competitividade e o acirramento do mercado pelo qual as empresas estão enfrentando, verifica-se que obter informações estratégicas, bem como ter acesso a estas informações por meios ilícitos ou tentar burlar um sistema de uma empresa estão se tornando práticas cada vez mais presentes da realidade organizacional.

A Intranet dispõe de um sistema de informações utilizadas por um grande número de usuários e suas permissões no que diz respeito ao acesso a elas é limitado. Porém, apesar das facilidades que oferece, um sistema que é baseado numa rede interna e em tecnologia típica da *web* não está totalmente seguro quanto a possíveis violações ou deturpações das informações que nele constam, em que ataques contra a integridade e autenticação podem vir a ocorrer.

Portanto, aspectos como os anteriormente citados e o interesse sobre sistemas de segurança na Intranet de uma organização como o TRT conduziram e motivaram o desenvolvimento deste trabalho. Afinal, um tema tão desafiador e que oferece tanta

resistência por parte dos informantes merece ser melhor explorado, para que se possam anexar contribuições significativas à gestão dos sistemas de informação, de modo geral, em especial aqueles ligados à segurança dos dados e informação da empresa. Neste sentido, verifica-se, neste trabalho de pesquisa, a possibilidade de contribuir com o referencial teórico sobre o tema em questão.

2 FUNDAMENTAÇÃO TEÓRICA

A complexidade e o surgimento de tecnologias informacionais têm influenciado a administração de empresas há muito tempo. A diferença agora, é que a velocidade dos avanços aumentou consideravelmente, o que tem propiciado um modelo de gerenciamento baseado na inovação.

As grandes mudanças incluem elementos como inovações tecnológicas e novas tecnologias de serviços baseados em computadores, globalização da concorrência e dos mercados. Assim, a questão da gestão da tecnologia tem como fundamento a maneira como as inovações nessa área devem ser gerenciadas a fim de melhorar a competitividade. Esse enfoque está produzindo grandes alterações no paradigma de administração.

O uso de novas tecnologias é percebido como ameaça e risco para as organizações durante processos de inovação tecnológica. Algo é novo para uma dada situação se puder ser visto como uma inovação mesmo que para outro local já seja considerado passado (Jacobsen *apud* Tornatzky e Fleischer, 2000).

A inovação tecnológica representa um meio eficaz para atuar no mundo dos negócios, no entanto pode produzir efeitos negativos e positivos. O administrador passa a ter um papel importante e deve considerar o ambiente em mudanças no qual atua.

Nesse contexto, as empresas são surpreendidas o tempo todo por um novo concorrente, pelo impacto da tecnologia da informação, pela globalização dos mercados, o que vêm provocando grandes mudanças organizacionais.

2.1 Mudança organizacional no contexto da inovação tecnológica

O ambiente de trabalho deve favorecer o processo da inovação, pois se for excessivamente rígido, dificilmente aparecerão novos projetos. Assim, as empresas

devem criar um ambiente de trabalho que favoreça os novos desenvolvimentos. Ainda, é fundamental que a alta gerência esteja comprometida com a inovação, embora muitas vezes esse espírito já esteja arraigado na cultura da empresa.

Sobre este aspecto, Montana e Charnov (1999) declaram que uma empresa pode estar integralmente comprometida com determinada forma de tecnologia e ter feito grandes investimentos de capital em máquinas e treinamento de pessoal, somente para ver emergir uma tecnologia inovadora e de menor custo.

Já para Wood Jr. (2002), o desenvolvimento de inovações gerenciais pode ser entendido pela interação de um conjunto conceitual de fatores contextuais, estruturais e organizacionais. Segundo o autor, as empresas que visam a inovação devem dar liberdade a seus colaboradores para incentivar comportamentos audaciosos, para que eles se sintam motivados a criar. Concomitantemente, o profissional envolvido com tecnologia precisa cada vez mais se engajar em um processo de permanente evolução de conhecimento no ambiente com o qual interage, de modo a se capacitar a uma condição de inovador de tecnologia. Não basta conhecer novas tecnologias, é preciso saber selecionar qual a mais adequada, em prol da melhoria da competitividade da organização.

A evolução da tecnologia, principalmente no que se refere aos recursos computacionais, vem impondo de forma generalizada uma nova concepção em termos de necessidades a serem atendidas.

Desse modo, as empresas vêm se adequando a capacidade de integração dessas tecnologias conduzindo a novos modelos de gerenciamento provocando mudanças que diferem de uma organização para a outra. Cada empresa tem seu caminho de transformação, diferenciado e singular. A atividade empresarial mais importante da atualidade consiste em conceber e desenvolver mudanças em grande escala, a fim de melhorar o nível de rendimento. Com relação a essa questão, existem quinze princípios pró-mudança, segundo um estudo realizado pela Price Waterhouse - firma de consultoria, (CARLOS & SALIBINETO, 2001), quais sejam:

a) enfrentar a realidade: a estruturação de uma empresa – produtos e serviços que oferecem e os processos e as tecnologias em que aqueles se baseiam – perde a validade em pouco tempo. Todos somos seduzidos igualmente pela idéia de

que o já construído continuará florescendo. No entanto, novos modelos de empresa surgem com freqüência cada vez maior e a competitividade do que já foi construído diminui;

b) agir sempre com a estratégia: o capital e a energia são limitados. Deve-se concentrar esforços de mudança somente nas áreas em que é possível obter maiores benefícios;

c) estabelecer comando firme: a mudança para se implementada precisa de comando enérgico. A responsabilidade é da alta administração, mas deve ser reforçada pelo cliente;

d) estabelecer um "clima de mudança": É necessário concentrar esforços na melhoria de rendimento dos setores mais importantes da organização;

e) dar informações convincentes: não se deve supor que todos estejam preparados para a mudança, o que é muito raro. É preciso um trabalho de comunicação constante e sincero, com relatórios freqüentes, para obter consenso;

f) fazer do cliente a mola mestra da mudança: o cliente deverá ser um aliado quando chegar o momento de argumentar a favor do projeto de mudança;

g) conhecer pessoas estratégicas: as mudanças constituem um centro de interesse para algumas pessoas e grupos poderosos. Será preciso dividi-los em segmentos, entender e atribuir prioridades às necessidades desses grupos;

h) comunicar-se continuamente: para o projeto obter sucesso, é necessário que se comunique constantemente a forma como as mudanças acontecerão. Se as mensagens forem claras, serão entendidas. Se forem concretizadas, terão credibilidade;

i) reformular o sistema de medidas: após o projeto ter sido elaborado, deve-se estabelecer um novo sistema de medidas coerente com as estratégias e os objetivos. O antigo sistema de medidas deve ser reavaliado e, se necessário, desativado;

j) utilizar todos os recursos: existem vários fatores fundamentais para provocar mudanças: os mercados e os clientes que se procura conquistar; a oferta de

produtos e serviços; a estrutura da organização; os processos em que se baseia a atividade da empresa e as tecnologias que os tornam possíveis. Uma mudança em grande escala só poderá ocorrer se todas essas alavancas funcionarem de forma coordenada;

k) ser a audacioso: o líder da mudança deve trabalhar sem descanso para convencer a equipe a pensar de modo audacioso e assim implementar inovações positivas na organização. O pessoal precisa sentir-se livre para abandonar os caminhos conhecidos, pensar por conta própria e trazer idéias novas à tona;

l) aproveitar a diversidade de recursos: atualmente, o número crescente de mulheres, minorias éticas e estrangeiros que trabalham nas empresas representa uma fonte sem-par de pensamento inovador;

m) desenvolver novas capacidades na empresa: em outras palavras , investir no capital humano, aumentando a competência profissional dos funcionários em todos os níveis . O esforço aqui é ampliar a competência técnica para a solução de problemas, a capacidade de tomar decisões e a liderança dos que trabalham nas trincheiras;

n) planejar : será preciso elaborar um plano de ação detalhado para impulsionar a mudança. Nele deverão ser especificadas todas as ações importantes: as mudanças nos processos, nos sistemas, nos funcionários, na cultura, no ambiente físico, na estrutura e nas necessidades de treinamento;

o) promover a integração de iniciativas: é vital manter uma base lógica integrada e coerente para todo o modelo de mudança. A apresentação de iniciativas sem planejamento apenas servirá para confundir os funcionários e diminuir o impacto positivo;

Diante do exposto, cabe ressaltar que avaliar criteriosamente os recursos a serem mudados é um importante passo quando se pensa em mudança. Afinal, a situação não será confiável até que a organização e seus colaboradores entendam o que é preciso alterar para implementar as idéias.

Quanto a este aspecto, Rodriguez e Ferrante (1995) consideram que as principais mudanças dentro das organizações serão do tipo cultural e comportamental. As mudanças consideradas do tipo cultural serão pelo uso intensivo de informações. Todas as organizações humanas, segundo Caruso (1999) desenvolvem uma cultura interna e qualquer elemento cultural novo que venha a fazer parte da cultura da organização é inicialmente tratado como elemento estranho. Já a mudança comportamental ocorrerá pela transferência de responsabilidades e sua *performance* dependerá muito da comunicação e integração.

Neste sentido, Day (2001) aborda que conseguir uma mudança bem-sucedida torna-se um desafio, pois a criação de um fato mais profundo no mercado frequentemente vai contra crenças arraigadas de cultura, estruturas, estratégias, aptidões e processos há muito vigentes. Mudanças ameaçam as pessoas, provocam resistências.

Contudo, de acordo com o autor, por mais que as iniciativas de mudança sejam difíceis de serem concluídas com sucesso, ficar parado talvez seja ainda mais arriscado. O ritmo de mudança está se acelerando, a concorrência crescendo, os clientes estão mais exigentes e novas tecnologias estão interferindo em estruturas de negócios tradicionais.

Os principais elementos da mudança organizacional, de acordo com Wood Jr.(*apud* BASIL & COOK, 2002, p. 21) são: tecnologia, o comportamento social, as instituições e estruturas. Para esses autores, a maioria das organizações muda em resposta às crises, sendo limitado o número de casos de atitudes proativas.

Ao considerar o comportamento social, elemento abordado pelos autores citados acima, Marchant e England (*apud* Oliveira, 1994, p.13) consideram as seguintes maneiras pelas quais as pessoas sentem-se afetadas pela tecnologia:

a) Ou a tecnologia é prejudicial, pois sugere:

- gasto de recursos;
- organização centralizada;
- perda de liberdade pessoal e dignidade;
- desigualdade e consumismo;
- trabalhos desqualificados;
- desemprego.

b) Ou a tecnologia é benéfica, pois sugere:

- maior liberdade pessoal;
- democracia participativa;
- mais tempo para recreação;
- maior conhecimento;
- melhoria na qualidade de vida.

A proliferação de novas tecnologias, cada vez mais presentes no dia-a-dia das pessoas apresenta mudanças tanto positivas quanto negativas.

Por isso, identifica-se uma interessante tipologia de análise para os ciclos de mudanças, apontada por Land e Jarman (*apud* WOOD JR., 2002, p 22), onde existem três fases de crescimento e mudança:

a) formação: o sistema descobre a si próprio e a seu mundo, organiza-se e cria um padrão de comportamento;

b) regulamentação: dá-se o crescimento por repetição do padrão e negação da diferença;

c) integração: o sistema ultrapassa a eficiência de seu padrão repetitivo. Para continuar a crescer, há uma redução na rigidez do padrão repetitivo e dos seus vínculos internos. Passa por uma fase de inovação, abertura e ruptura.

A mudança organizacional caracteriza-se assim, como um processo de melhoria contínua, cujo impacto das inovações tecnológicas conduzem as empresas a adotar novas formas de trabalho, renovando práticas administrativas. Dessa forma, vale analisar neste trabalho com maiores detalhes aspectos relativos a essa modalidade tecnológica.

2.2 A importância da tecnologia na empresa

A maioria das informações de uma empresa está normalmente concentrada e processada em computadores. Bens, pessoas e serviços são controlados por sistemas de informação processados pelos computadores.

O conceito geral de sistema pode ser caracterizado, segundo Melo (1999), como todo e qualquer sistema que apresente informações de entrada visando gerar informações de saída. A expectativa de se obter tais informações, para satisfazer determinadas necessidades, corresponde ao objetivo geral dos sistemas de informação.

Muitas empresas, públicas ou privadas, ainda se utilizam de grandes centros de processamento de dados, interligando os terminais e microcomputadores. Os grandes centros de processamento (CPD's) continuam e continuarão a existir, agora operando como centrais de processamento, possibilitando que cada área de negócio da empresa, cada uma de suas divisões, tenha domínio e possa processar os seus sistemas de modo independente.

Já especificamente as organizações públicas possuem características que as diferem das organizações do setor privado, desde a forma de gestão até o tipo de serviços oferecidos. As características peculiares à organização pública influenciam, inclusive, no desenvolvimento, implantação e utilização dos sistemas de informação, cuja importância tem crescido em virtude da análise estratégica e planejamento de órgãos governamentais (TAIT,2000).

Diante do exposto, Cassarro (1997) relata que a aplicação das técnicas utilizadas na Internet como os recursos técnicos proporcionados por "softwares" navegadores, gerenciadores de telecomunicações e pesquisadores de bancos de dados, passam a ser realizadas internamente às empresas, constituindo as intranets.

Para Chiavenato (2003) a Internet, a intranet, bem como, utilização do computador para integrar processos internos e externos estão modificando com uma rapidez incrível o formato organizacional e a dinâmica das organizações. A virtualização crescente das organizações é decorrência disso. O desafio reside na busca incessante de novas soluções e

a essência da eficácia está se deslocando para a busca de redes e parcerias em conexões virtuais dentro de um contexto ambiental mutável.

2.3 Intranet: conceito e finalidade

A intranet de uma empresa utiliza as tecnologias da Internet dentro da própria empresa: a manipulação das informações da empresa no formato *html (web),* o padrão de correio eletrônico (smtp), o sistema de troca de arquivos pelo sistema ftp, entre outros padrões de tecnologias emergentes da Internet. Todos esses serviços, ou programas, executam em conjunto com o protocolo tcp/ip.

A Internet, segundo Evans (1998) usa protocolos para permitir uma comunicação entre os dispositivos conectados. O protocolo central da Internet é o tcp/ip e cada computador conectado à Internet deve usar tcp/ip para se comunicar com o resto da Internet. A rede tcp/ip permite não apenas a conexão entre computadores locais, mas também entre redes. Essas conexões criam inter-redes (Internets) que fazem com que os usuários vejam os computadores de todas as redes interligadas como parte de uma única e enorme inter-rede. De acordo com Evans (1998), a mesma capacidade de compartilhamento foi ampliada daquela existente entre as máquinas de uma única rede para todos os sistemas de todas as redes conectadas.

Com o crescimento do número de usuários da Internet, as empresas iniciaram um processo de comércio pela grande rede. Atualmente realizam-se compras e vendas de produtos e serviços pela Internet. Além disso, o setor público vem paulatinamente se integrando à rede mundial como meio de disponibilizar e trocar dados com seus clientes internos e externos.

Neste sentido, uma intranet, para Starlin e Novo (1998), seria assim uma rede de uma empresa que utilizaria as tecnologias da Internet dentro da própria empresa: a manipulação das informações da empresa no formato *html* (*web*), ou padrão de correio eletrônico smtp, o sistema de troca de arquivos pelo sistema ftp, entre outros padrões de

tecnologias emergentes da Internet. Todos esses serviços, ou programas, executam em conjunto com o protocolo tcp/ip.

As intranets, segundo Stewart (1997), são soluções de rede completas que oferecem gerenciamento de informações que a organização necessita utilizando processos e protocolos Internet. As intranets até o final de 1995 eram chamadas internets empresariais – versões em miniatura privadas ou corporativas da Internet. Os dois termos fornecem informações descritivas sobre a intranet, palavra derivada de intra e *network* (rede), significando uma rede interior, semelhante ao termo Internet, que é uma palavra derivada de interconexão e *network*. Embora o termo Internet empresarial seja mais descritivo, o rótulo intranet é usado porque está mais próximo do termo Internet.

Nestes termos, Stewart (1997) afirma que uma das finalidades do uso da intranet está em produzir bens e serviços de modo a tornar disponíveis informações para pessoas que estão fora do ambiente organizacional. Em contrapartida o autor salienta que a primeira *web* era uma intranet projetada para distribuir informações dentro de uma organização, para as pessoas da própria organização.

Quando uma empresa instala um servidor *web* ao público-alvo envolve um ou mais dentre os seguintes públicos que estão fora da organização: o público em geral, clientes atuais e futuros, acionistas, e até mesmo os concorrentes.

Quanto ao projeto e layout da intranet abrangem as finalidades a seguir, consideradas por Stewart (1997):

a) Fornecer aos clientes informações sobre seus benefícios trabalhistas;

b) dar aos clientes acesso a bancos de dados pesquisáveis com informações e suporte técnico de hardware e software para PCs;

c) fornecer aos clientes uma interface de browser *web* com o banco de dados de estoque e de pedidos da corporação

d) usar a tecnologia *web* para permitir aos clientes o compartilhamento de arquivos de dados a partir de aplicativos comuns.

Considerando o projeto lógico de uma intranet, o autor afirma que o projeto lógico e o layout são processos para a disposição das informações na intranet, segundo algum plano geral. As informações que se planeja colocar na intranet são naturalmente decompostas em

seções lógicas. Logo, se pode refletir estas divisões naturais em um projeto lógico. Finalmente, tendo o projeto é importante avaliar e definir o grupo de usuários, bem como, a segurança dos que terão acesso à intranet.

2.3.1 Público da intranet

A intranet está dirigida para as pessoas que trabalham na empresa. Assim o público alvo será imediatamente definido, alega Stewart (1997), como o grupo de usuários que detém algum tipo de acesso à intranet. Essa não é uma definição do público real, mas sim do público em potencial. Ainda é preciso dividir esse público com base em suas características comuns. O tipo de trabalho que um grupo de pessoas executa pode ajudá-lo a definir suas necessidades como clientes da intranet. Os cientistas e engenheiros formam um grupo completamente diferente, com interesse maior em usar a *web* em seu trabalho. Entretanto ambos os grupos fazem parte do público geral que são funcionários da empresa, com interesses nas informações e serviços prestados pelos departamentos de Recursos Humanos e/ou Almoxarifado e Logística .

No entanto, o gerenciamento de pessoas que utilizam a intranet não é considerado fácil. Se as pessoas nunca precisassem acessar o sistema, eliminar-se-ia 99% dos problemas a serem enfrentados. Há medidas que auxiliam a reduzir a dificuldade dessa tarefa e ainda evitar alguns dos maiores problemas relacionados ao usuário. A solução mais efetiva segundo Stewart (1997) é o treinamento. Os usuários precisam ser treinados e informados quanto aos seguintes fatos:

a) Que operações estão além do escopo da intranet ou de seu acesso, como grandes downloads, instalação de novos softwares, multimídia e videoconferência pela Internet;
b) O que significam realmente os vários níveis de acesso de segurança;
c) Que áreas de dados são públicas, restritas ou disponíveis apenas a certas pessoas, grupos ou participantes do projeto;

d) Os programas de manutenção para todas as áreas da intranet, especialmente aquelas que afetam os usuários;
e) Como distinguir um problema real de software ou hardware de um erro humano ou atraso no sistema;
f) Como informar problemas e erros para o técnico apropriado;
g) Quem é responsável por cada dispositivo de hardware e pacote de software;
h) Como submeter pedidos para alterações, acréscimos ou cancelamentos de serviços;
i) Como instalar e testar *softwares* clientes;
j) Como proteger seus dados contra vírus, exclusão, mudança de local ou outros danos;
k) Como a intranet está organizada e por quê;
l) Onde cada periférico significativo está localizado, quem tem acesso, porque o acesso é limitado, como operá-lo e como informar problemas;
m) Quem é responsável pelos dados da organização;
n) Como auxiliar os administradores do sistema na manutenção de uma intranet operacional de sucesso;
o) A política da empresa para todos os dados na intranet;
p) Quaisquer diretrizes, parâmetros, limites, restrições e outras limitações impostas ao hardware, software, usuários e dados.

Quanto mais informados estiverem os usuários, mais proveito pode-se tirar do conhecimento e habilidade na manutenção da intranet e na prevenção e relato dos problemas. Os usuários que entendem que não podem tentar uma ação restrita ou perigosa provavelmente pedirão ajuda em vez de impor a sua vontade sobre o sistema. Por isso, o responsável pela segurança deve certificar-se de que os usuários estejam informados. Além disso, é importante treinar os funcionários também para pedir ajuda e instrução.

Ao iniciar o projeto de uma intranet, o primeiro passo deve ser a definição exata do público-alvo, ou clientes. Os serviços de informação contidos na página devem estar dirigidos principalmente a esses clientes. A atividade principal de uma empresa pode ser a fabricação de rolamentos, o fornecimento de serviço de seguro saúde ou o pagamento de

benefícios do governo, mas os clientes da intranet não são os mesmos que compram ou recebem estes produtos e serviços.

Nesse caso, os clientes são as pessoas da própria empresa, que tornam disponíveis esses produtos ou serviços. A partir da definição do público-alvo pode-se projetar uma intranet e saber quais informações ela conterá. Dessa forma, a empresa pode fornecer, conforme Stewart (1997), serviços de um ou mais tipos para seus funcionários (clientes). Esses serviços podem ser muito diversos:

a) Serviços de recursos humanos: Independentemente da empresa possuir ou não um departamento de recursos humanos formal, há uma grande quantidade de papel envolvida, e boa parte contém informações que os funcionários necessitam. Entre elas são:

- manuais de funcionários, códigos de conduta, informações sobre planos de seguro-saúde, férias e salários, procedimentos para a compra de produtos ou reembolso de despesas e assim por diante;
- quadros de avisos da empresa repletos de informações do governo sobre salário mínimo e políticas previdenciárias, anúncios de emprego, horário de trabalho, cursos de treinamento, menus de lanchonetes, horários de torneios esportivos, anúncios de pneus usados à venda e centenas de outros;
- cartões de ponto de funcionários, informações vitais (estado civil, endereço residencial) avaliações de desempenho;
- boletins informativos com anúncios da empresa e outras comunicações;
- todos os diversos documentos e procedimentos que um departamento de recursos humanos utiliza para contratar, demitir, promover, transferir, treinar, registrar e gerenciar o emprego e os benefícios dos funcionários;

b) Serviços materiais e logísticos como o espaço nos escritórios, equipamentos (mesas, telefones, computadores, maquinário), suprimentos e todos os serviços físicos envolvidos na operação da organização;

c) Serviços de sistemas de informação.

De fato, a maioria das empresas tem uma organização formal e informal que reflete serviços com departamentos como almoxarifado e logísticos, recursos humanos, sistema

de informação, e outros departamentos similares que prestam serviços aos funcionários. Observá-los é o primeiro grande passo para definir o conteúdo e o layout da intranet da empresa.

Outras fontes de informação e serviço que a intranet pode oferecer, conforme Stewart (1997) são:

a) uma lista pesquisada por meio da *web* de itens em excesso, como o mobiliário, equipamentos de computação, ou maquinário, que pode economizar muito dinheiro em uma empresa grande, permitindo otimizar sua utilização a ociosidade;

b) mapas em imagens que podem ser clicadas de plantas do edifício que o pessoal de manutenção pode estudar com um detalhamento cada vez maior. Válido para as plantas de engenharia de instalações e equipamentos industriais, além de todas as instalações subjacentes (água, eletricidade, aquecimento, conexões de rede);

c) de maneira similar porém menos detalhada, mapas em imagens que compõem uma *front-end* gráfica da lista telefônica da empresa, que permite aos funcionários se localizarem com facilidade. Dar um clique sobre um prédio no mapa do campus pode trazer a lista telefônica daquele edifício, dar uma clique em uma sala pode trazer o nome de seus ocupantes;

d) uma ampla gama de formulários a serem preenchidos para localizar e atualizar estoque, fazer pedidos, localizar e requisitar suprimentos, manter os registros adequados e centenas de outras tarefas.

Diante das informações disponibilizadas numa intranet, algumas fontes de recursos são citadas por Stewart (1997):

a) Se o uso do computador é generalizado na empresa, pode-se ter pessoal de *help desk* que atenda a telefonemas de usuário respondendo a questões sobre *software* , *hardware* e outros assuntos relacionados. As pessoas que operam o serviço telefônico sabem que há perguntas que são repetidas diariamente e que têm a mesma resposta. As respostas pré-preparadas a perguntas comuns podem formar o corpo central de um *help desk* na intranet. Com o *Netscape*

ou outro *Browser* os funcionários da empresa podem usar formulários a serem preenchidos como os do *Yahoo* ou *lycos* para procurar respostas (e criar novos formulários.). Dando um passo adiante, não há motivo pelo qual não seja possível tornar disponível para os usuários os serviços do *help desk*, permitindo que eles procurem as informações que necessitem sempre que for preciso.

b) Interfaces baseadas na *web* para aplicativos tanto comerciais como domésticos estão disponíveis. Independentemente da finalidade do banco de dados, ele tem duas funções principais: incluir ou atualizar informações e recuperá-las. Mesmo que o aplicativo de banco de dados tenha telas especiais para que os usuários executem funções, ambas podem ser feitas com formulários preenchidos por meio da *web* e de *scripts backend* CGI que acessam o banco de dados. A vantagem para os usuários é a visão de uma interface confortável e reconhecida implementada para múltiplas finalidades.

c) Documentos existentes em processadores de textos, planilhas, e outros aplicativos podem ser compartilhados usando tecnologia *web*. A configuração apropriada do servidor *web* e dos browsers de seus usuários permite que um executivo da empresa dê um clique em um *hiperlink* e acesse os dados operacionais ou de vendas diretamente de seu programa de planilha para análises e projeções e então grave os resultados para inclusão em apresentações ou documentos em processadores de texto.

d) Cientistas, engenheiros e técnicos podem compartilhar arquivos de dados a partir de seus aplicativos em sua intranet. Químicos podem rodar programas de modelagem molecular apenas dando um clique em um *hiperlink* e apontando para um arquivo de dados; engenheiros podem acessar arquivos CAD da mesma forma.

e) É possível instalar um aplicativo personalizado inteiro, que a empresa utiliza em uma interface *web* tendo o *Netscape* como sua interface e com uma ajuda embutida para seus usuários.

As intranets são consideradas entre outras coisas como um meio para colaboração entre os setores de uma empresa através do compartilhamento de informações. A seguir são apresentadas algumas de suas vantagens e desvantagens.

2.3.2 Vantagens e desvantagens de uma intranet

A decisão de adotar ou não uma intranet na organização inclui se ela oferecerá retorno adequado ao investimento nas áreas de *hardware*, *software*, treinamento, conversão de conteúdo e manutenção.

De acordo com Stewart (1997) as intranets são ferramentas e não máquinas de dinheiro. Quando usadas corretamente podem acelerar a comunicação e a troca de informações e melhorar a qualidade e a quantidade de bens e serviços de uma organização.

Neste sentido, Evans (1998) afirma que a intranet foi projetada para distribuir informações dentro de uma organização, para as pessoas da própria organização. Ou seja, a idéia é divulgar informações corporativas ou vender coisas por intermédio da *web*.

Uma intranet é uma rede privada que incorpora os protocolos, processos e padrões encontrados na Internet.

Mais do que apenas um híbrido de tecnologias de rede e Internet, a intranet aprimora as capacidades de ambas. Assim, de acordo com Stewart (1997) alguns dos benefícios desta rede são:

a) A capacidade de enviar informações rapidamente;

b) Facilidade em aprender e usar;

c) Expansível;

d) Sem limite de usuários simultâneos;

e) Totalmente testada e implementada no mundo inteiro;

f) Comunicações privadas seguras;

g) Controlável;

h) Pouco dispendiosa.

Ainda vale lembrar que as intranets combinam o melhor das redes e dos sistemas de informações tradicionais com a arquitetura aberta e os serviços de informação da Internet.

Para Albertin (2000), as intranets têm vantagens óbvias, porém oferecem também desvantagens. Algumas das vantagens são:

a) Fácil publicação de informação;
b) Custo;
c) Facilidade de uso;
d) Baixa manutenção;
e) Escalabilidade;
f) Fácil distribuição de software.

Nesse contexto, pode-se apontar como principais desvantagens as que seguem:

a) As aplicações colaborativas para intranets não são tão poderosas como as oferecidas por *groupware* tradicional;
b) Risco a curto prazo;
c) Menor integração com a *backend.*

Considerando a tecnologia *web* interna e a apresentação das suas vantagens evidentes Stewart (1997) enquadra as vantagens nas três categorias a seguir:

a) Plataforma Universal: as *webs* fornecem uma plataforma comum para localizar, recuperar, exibir e atualizar uma variedade de informações, que abrangem dados numéricos em bancos de dados relacionais e documentos compostos de texto estruturado, imagens e até mesmo objetos multimídia, como áudio e imagens animadas;
b) Modo de exibição unificado: as *webs* ajudam a organizar às informações através da apresentação de diversos tipos de dados em um estilo padrão. Em um navegador *web*, a variedade de elementos da comunicação empresarial tradicional – relatórios, artigos, memorandos e tabelas – assume uma aparência e um comportamento comuns. Além de apoiar e agilizar a tomada de decisão, os padrões podem reduzir a curva de aprendizagem do novos aplicativos;

c) Língua franca: a tecnologia *web* baseia-se em padrões flexíveis e universalmente aceitos. Por isso, as intranets podem acessar informações armazenadas em sistemas existentes sem implicar em uma programação de alto custo. Isso valoriza o seu investimento atual na rede, o que constitui uma vantagem em relação às tecnologias patenteadas, que costumam exigir a substituição integral das ferramentas existentes.

2.3.3 A diferença da intranet em relação às redes privadas

A intranet é uma mistura de redes privadas tradicionais com a Internet, bem como uma nova entidade própria. O exame dessa rede, sob várias perspectivas, torna essa distinção mais evidente.

As diferenças entre uma intranet e uma rede privada tradicional são numerosas, incluindo variações nas tecnologias básicas, aplicativos disponíveis e métodos de gerenciamento de informações.

Para Stewart (1997), a diferença tecnológica mais evidente é o protocolo principal e central do tcp/ip. Até pouco tempo, o *NOS* empregado em uma rede privada que não se comunicava com a Internet era qualquer coisa diferente de tcp/ip. O tcp/ip, embora seja um protocolo consistente, exige maior poder de computação do que a maioria dos *NOSs*, sendo constantemente desprezado em conseqüência do pequeno aumento dos custos em *hardware* de maior potência. As intranets usam tcp/ip para tirar proveito dos muitos benefícios que ele tem a oferecer.

As redes padrão forçam os usuários a aprenderem vários aplicativos, cada um com interfaces próprias, protocolos particulares e geralmente com técnicas de programação difíceis de dominar. Essa curva de aprendizado gera uma aceitação lenta quando novos produtos são introduzidos no sistema de informação.

A maioria dos aplicativos preparados para rede é cara, especialmente em comparação com as versões para intranet/Internet de produtos semelhantes. Os softwares

para rede geralmente possuem limites para o número de usuários simultâneos e não podem compartilhar dados entre os aplicativos. Os aplicativos para intranet normalmente usam interfaces iguais ou semelhantes, protocolos padronizados e técnicas de programação fáceis de serem dominadas. A padronização dos principais serviços de informação permite que a habilidade adquirida em um serviço seja facilmente aplicada a outros serviços.

As redes padrão geralmente são forçadas a confinar seu ambiente de computação a uma única plataforma de computador, e às vezes são limitadas a sistemas operacionais específicos e aplicativos relacionados. O uso de um padrão de protocolo totalmente compatível e mundial na intranet, o tcp/ip, permite que diversas plataformas, *OSs* e aplicativos convivam de forma produtiva em uma única rede.

As redes padrão limitam o número e o tipo de aplicativos e serviços disponíveis a seus usuários. As intranets podem se beneficiar com qualquer avanço, desenvolvimento ou melhoria feita a quaisquer produtos que operem pelo protocolo tcp/ip. Assim, as redes padrão geralmente são limitadas ao método de gerenciamento de informações oferecido pelo uso isolado de uma ferramenta de gerenciamento de informações e comunicações (semelhante ao *Lotus Notes*). As intranets permitem que diversas ferramentas de gerenciamento sejam usadas paralela e coletivamente de uma forma mutuamente produtiva.

2.3.4 Implementação da infra-estrutura da intranet

A infra-estrutura básica de hardware e software necessária para implementar a intranet na empresa de acordo com Evans (1998) é:

a) rede tcp/ip: são protocolos fundamentais da rede Internet. Somente os protocolos tcp/ip, o fundamento da Internet mundial, oferecem suporte a *web* em redes de áreas locais e mais amplas , incluindo a Internet e a sua rede local. Para instalar a intranet é preciso rodar a rede tcp/ip;

b) hardware para o servidor *web:* praticamente não há limite para a seleção de um sistema de computação no qual rodar um servidor *web.* Quase todos os computadores modernos equipados para rede, incluindo o programa de rede tcp/ip, podem abrigar um servidor *web* . O sistema mais usado para servidores *web* são máquinas *Unix* como os servidores ou instalações de trabalho *Sun, IBM, Digital e Hewlett-packard.* A seleção do hardware que atuará como servidor da intranet depende de vários fatores, incluindo o nível de tráfego previsto, a facilidade de instalação, os conhecimentos técnicos disponíveis na empresa e outras exigências;

c) programas para o servidor *web:* o principal servidor *web* comercial para sistema *Unix* é o *Netsite* da *Netscape Communications,* fabricante do *browser web netscape navigator;*

d) processadores *html* e ferramentas: é possível criar páginas *web* com a linguagem de marcação de hipertexto (*html*) usando qualquer processador de texto. Como os documentos *html* são textos puros *ascII* com códigos *html* simples, não é necessário usar um processador *html* especializado ou uma ferramenta de conversão;

e) browser *web*: *o ncsa mosaic e o netscape navigator* são dois pacotes de *browers web* mais conhecidos . Ambos estão disponíveis para *Windows, mac,* e para uma ampla gama de sistemas U*nix;*

f) aplicativos auxiliares comuns de *browers* da *web* : são aplicativos que podem ser carregados com o *browser web;*

g) outros serviços acessados via tecnologia *web*: além das muitas possibilidades de aplicativos auxiliares para a intranet, há variedade de serviços de rede baseados no tcp/ip possível de integração à intranet;

Mesmo sendo estes serviços comumente vistos como serviços da Internet, não há motivo pelo qual não se deva implementá-los e usá-los localmente como parte da intranet, mesmo se a empresa não estiver conectada à Internet.

Considerando o avanço na área de serviços de informações, Stewart (1997) aborda o protocolo tcp/ip e os principais benefícios que advém da sua utilização; quais sejam:

a) TCP/IP: é o principal protocolo de uma intranet, assim como é o principal protocolo da Internet. Em uma intranet, o tcp/ip não precisa ser o único protocolo, mas deve ser totalmente ativo e disponível a cada cliente e servidor na rede (seja por meio de um gateway de software ou hardware). O objetivo dessa centralização em torno do protocolo tcp/ip é aproveitar o sistema de transporte de comunicações na rede fornecido por ele. Os benefícios advindos do uso do tcp/ip na Internet também podem ser utilizados por intranets;
b) Troca de pacotes: um método veloz de endereçamento e remessa, especialmente quando comparado aos mecanismos de remessa tradicionais de chaveamento de circuito;
c) Transporte independente do conteúdo: o tcp/ip pode transmitir dados e saída de outros protocolos, independente do conteúdo; assim, muitos sistemas de remessa de dados especializados podem ser empregados;
d) Remessa de dados confiável: como o esquema de remessa tcp/ip não se baseia em qualquer conexão isolada na rede, a remessa de dados é mais confiável em conseqüência do redirecionamento automático ao serem encontrados vínculos inoperantes;
e) Suporte para compactação e criptografia: o fato de ser irrelevante para o conteúdo permite colocar algoritmos complicados de compactação e criptografia em uso nos dados transmitidos para reduzir o tempo de transferência, aumentar a privacidade e garantir ainda mais a remessa para o destinatário apropriado;
f) Totalmente escalável: o tcp/ip pode dar suporte adequado a uma rede de duas a vinte milhões ou mais de máquinas;
g) Usuários simultâneos sem limite: o protocolo não possui limitação para o número de usuários concorrentes;
h) Compatibilidade: o tcp/ip é comparável com quase todas as plataformas de computador e os modernos *OSs* e *NOSs* (sistemas operacionais de rede), seja pelo suporte nativo direto ou pelos *softwares* ou *hardware* de *gateway* suplementar;

i) Solução a longo prazo: o tcp/ip está e continuará a estar na Internet. A versão pode mudar e suas capacidades podem ser aumentadas e expandidas , mas o tcp/ip veio para ficar;

j) Padrões abertos: o tcp/ip é um protocolo que pertence à comunidade de usuários; cada indivíduo e fornecedor tem acesso completo a todas as especificações e parâmetros com a finalidade de desenvolver novos produtos totalmente compatíveis com tcp/ip.

Nesse contexto, vale destacar que uma desvantagem significativa do tcp/ip, de acordo com Stewart (1997) é a maior demanda na potência geral do sistema e a *RAM* necessária a cada dispositivo da intranet. O tcp/ip é um protocolo resistente e confiável, mas esses recursos valiosos exigem um pouco mais de poder de computação. O tcp/ip envolve gastos em recursos extras para obter mais memória, sendo diretamente recompensado em velocidade, confiabilidade e desempenho. Um dos protocolos utilizados na rede para uso de outras pessoas é o ftp que será abordado a seguir.

2.3.4.1 Instalação de protocolo de ftp

File transfer protocol é o protocolo usado para transferência de arquivos na Internet. O ftp é um conjunto de comandos tipo *Unix* para acessar computadores por toda a Internet, listar arquivos, mudar diretórios e copiar arquivos para o computador.

Sobre este protocolo Baran (1995) define como arquivos documentos legais até jogos de computador que residem em instalações (o jargão da Internet para computadores) de ftp por toda a Internet. Alguns deles são inacessíveis ou acessíveis somente a certos indivíduos qualificados. Outros estão disponíveis a todos os usuários gratuitamente. Dependendo da natureza da conta na Internet, é possível colocar arquivos em certos locais de ftp para uso de outras pessoas.

Se a intranet envolve uma rede de longa distância (*wan*) com *links* lentos entre os locais remotos, os clientes podem cansar-se de esperar que as transferências ftp iniciadas

pelo *browser web* se completem. O *ftpmail* oferece uma solução possível para esse problema, apesar da interface ser um retorno ao ftp linha de comando; convém contorná-lo. A única conexão de certas intranets com o mundo externo é pelo correio eletrônico, por motivos de segurança ou outros. Nessa situação, o *ftpmail* pode ser a única maneira de recuperar arquivos de servidores ftp anônimos no mundo externo. Os usuários enviam mensagens de correio eletrônico contendo comandos para um endereço de *ftpmail*; o programa responde a estes comandos enviando de volta uma mensagem de correio eletrônico contendo os resultados dos comandos, inclusive arquivos. Os comandos enviados para o *ftpmail* são comandos ftp normais, como os digitados por um usuário no ftp de linha de comando baseada em texto. O resultado é que os usuários que não sabem como usar essa interface terão de aprender.

A utilização do *ftpmail* na intranet pode ser aplicada ao correio eletrônico. Eis apenas algumas utilidades conforme Stewart (1997):

a) Os usuários podem comunicar-se usando *browsers web* para enviar e ler mensagem de correio eletrônico por meio das listas de distribuição da intranet;

b) Mensagens de correio eletrônico enviadas para listas de distribuição podem ser arquivadas e indexadas para subsequentes busca e recuperação usando um *script* para índices;

c) A transferência de arquivos por meio de enlaces lentos de redes de longa distância pode ser enfileirada para rodar assincronamente usando-se *scripts*, permitindo um uso mais eficiente da largura de banda da rede.

Outro ponto a ser considerado quando da implementação da estrutura da intranet e que será abordado adiante é a *Common Gateway Interface – CGI* .

2.3.4.2 Cgi e intranet

A conexão de um computador ao mundo externo oferece riscos em potencial à segurança e podem ser explorados por alguém com más intenções. Ao instalar um servidor *web* Weinman (1997) admite que: " ...você explicitamente convida um tipo de entrada enquanto simultaneamente tenta impedir invasões indesejadas" (1997, p.245).

Contudo, os aplicativos cgi podem ser considerados como extensões da funcionalidade básica de um servidor www, executam tarefas de processamento específico de informações, carregamento e formatação, para apoiar os seus servidores www. Nestes termos, Gaither, Hassinger e Erwin (1996) definem a interface cgi como uma maneira de o servidor da *web* acomodar programas e serviços adicionais, que poderão ser usados para acessar aplicativos externos, de dentro de qualquer documento ativo da *web*. O termo *gateway* (passagem, portal) descreve o relacionamento entre o servidor www e os aplicativos externos que controlam o acesso aos dados e as rotinas de manipulação para o mesmo.

2.3.5 Intranet e correio eletrônico

O correio eletrônico, para Benett (1997), é a mais simples das técnicas de envio/recebimento de mensagens utilizadas nas empresas modernas e, por isso mesmo, é também uma das mais eficientes e duradouras. A maioria das empresas depende de colaboração, e o correio eletrônico facilita o diálogo que possibilita a interação e troca de idéias e informações.

Um sistema de correio eletrônico permite assim, que pessoas de uma rede enviem mensagens uma às outras. Parte das vantagens do sistema provém da capacidade de entrar em contato com qualquer pessoa da rede. Outra característica que o correio eletrônico atribui à comunicação é a capacidade de deixar mensagens em uma caixa de correio. Os

destinatários não precisam estar operando seus computadores quando alguém lhes envia uma mensagem.

Ainda, com relação as vantagens da presença do correio eletrônico, Tanenbaum (1994) equipara a velocidade do correio eletrônico com a do telefone sem exigir que as duas partes estejam disponíveis no mesmo instante e possibilita uma cópia escrita da mensagem e sua transmissão a muitas pessoas de uma só vez.

Uma diferença apontada por Tanenbaum (1994) entre o correio eletrônico e a transferência de arquivos de uso geral é que as mensagens de correio são documentos altamente estruturados. Em muitos sistemas, cada mensagem apresenta o nome e o endereço do transmissor, o nome e o endereço do destinatário, a data, hora da postagem, nível de segurança além do seu conteúdo.

O correio eletrônico, segundo Crumlish (1995) é frequentemente utilizado para:

a) rodar o programa de correio;
b) enviar o programa de correio;
c) enviar correspondência;
d) salvar à correspondência em uma pasta;
e) responder à correspondência;
f) passar adiante a correspondência;
g) eliminar correspondência;
h) salvar correspondência;
i) sair do programa de correio.

E-mail ou correio eletrônico é uma das mais antigas formas de comunicação em rede entre os indivíduos. Para Stewart (1997) é também uma ótima técnica para distribuir informações, por meio do uso criterioso de listas de correspondência e especialmente servidores de lista de correspondência, e também o tipo mais popular de software para rede. Trata-se, em verdade, do formato eletrônico de carta escrita que permite aos usuários a transferência de mensagens, memorandos, notas, arquivos de imagem, arquivos de som, aplicativos para outros usuários em uma rede.

Quanto ao servidor de correio eletrônico de uma intranet típica usa o protocolo tcp/ip para enviar e acessar correspondência. No entanto, se seus usuários não precisarem acessar

a Internet, outros protocolos (como ipc/spc ou *netbeui*) também poderão ser usados para acessar a correspondência do servidor.

O número de usuários não é um fator real para determinar se uma empresa pode se beneficiar com o correio eletrônico. Na realidade, qualquer empresa cujos funcionários precisem trocar mensagens pode se beneficiar com esse meio de comunicação. Além disso, ele permite que sejam enviadas mensagens com arquivos anexados para outras pessoas, que poderão utilizar esses anexos de várias maneiras.

O correio eletrônico, de acordo com Stewart, é baseado em três tipos básicos: estação de trabalho, servidor único e em vários servidores, descritos a seguir.

2.3.5.1 Tipos básicos de correio eletrônico

De acordo com Stewart (1997) existem três tipos básicos de correio eletrônico:

a) Correio eletrônico baseado em estação de trabalho: enviado ponto a ponto, correio de grupo de trabalho só precisa de um *software* cliente em cada espaço de trabalho. Normalmente, um usuário configura seu computador como agência de correio e permite que outros se conectem a ele para enviar e receber correspondência;

b) Correio eletrônico baseado em servidor único: permite que os usuários conectem-se ao servidor de correspondência e enviem e recebam mensagens. Como o servidor está sempre funcionando e geralmente em uma área protegida, esse esquema tem o benefício da segurança em relação ao correio baseado em grupo de trabalho;

c) Correio eletrônico baseado em vários servidores: permite manter o servidor de correio local, com servidores de correio replicando dados em segundo plano. Esses servidores podem ser administrados a partir de um local central ou a administração pode ser compartilhada com uma empresa.

O correio eletrônico, conforme Stewart (1997), é considerado um dos fundamentos da comunicação na estrutura da Internet. Contudo, ele também pode se tornar uma fonte de sérios riscos e problemas legais para uma empresa. Assim como ao navegar pela *web*, um bom método a ser utilizado é regular o uso da intranet por meio de uma política de uso aceitável que defina os limites de uso de correio eletrônico pelo funcionário.

Ainda, a maioria das empresas acredita ser proprietária da correspondência eletrônica trocada por meio de suas intranets. Embora os funcionários possam estar cientes do fato de que suas ações estão sendo acompanhadas, não só é possível que uma empresa monitore a atividade do funcionário por meio de uma intranet como também é legal.

2.4 Segurança em informática

A segurança dos sistemas é sempre um desafio relata Stewart (1997) e nunca houve e dificilmente haverá, num futuro previsível, um sistema de controle interno que proporcione cem por cento de proteção contra fraudes, prejuízos e ações dolosas. Todo e qualquer sistema pode ser fraudado, violentado, basta que somem esforços para descobrir e explorar brechas para entrar em qualquer sistema e manipular suas informações retrata o autor. Portanto, para se ter segurança é preciso realizar a aplicação de recursos. Nesse contexto, algumas das providências, segundo Cassarro (1997) que devem ser analisadas, estudadas e implementadas são:

a) utilizar barreiras contra fogo (*firewalls*) para proteger os equipamentos principais e os servidores e, quando for o caso, alguns ou todos os micros;
b) utilizar apenas programas (*softwares*) que exijam o emprego de senhas (*password*);
c) validar os dados automaticamente, quando de sua entrada no sistema. Ao se completar a digitação de um campo, este deve ser, de imediato, automaticamente aceito ou rejeitado pelo sistema;

d) operar com programas que procedam à geração automática de cópias para fins de segurança (*Backup*);

e) chavear, desligar os equipamentos quando seus operadores não estiverem na área, dificultando seu uso indevido;

f) empregar criptografia (combinações geradas por matrizes matemáticas) para "esconder" os dados a serem transmitidos via redes, notadamente a Internet;

g) fazer uso de chaves (senhas) e proceder a sua substituição, freqüente e aleatoriamente.

Estas são algumas das providências que proporcionam o mínimo de proteção e contribuem para a integridade das informações de cada sistema.

Segurança em informática é parte integrante da segurança empresarial e ambas utilizam conceitos e abordagem administrativa, técnica e operacional comuns.

Segundo Gil (1994), metodologias, práticas, instrumentos e produtos identificam-se entre segurança empresarial e de informática. Porém, forma, intensidade e prioridades podem ser tratadas de maneira distinta quanto ao risco, contempladas pela tecnologia, plataformas e sistemas de informática. Ainda, de acordo com o autor, a segurança em informática pode ser definida, como participante da responsabilidade de todos os profissionais das organizações envolvidas com a tecnologia computacional direta ou indiretamente.

Desta forma, o cumprimento das normas, procedimentos e práticas de segurança, assim como o atendimento de metas de segurança responsabiliza usuários e profissionais de informática. Considerando o exposto, no que se refere a execução da segurança em informática, Gil (1994) aponta situações de insegurança consoante os momentos relacionados:

a) **logs** com as operações ocorridas quando da utilização das plataformas de informática;

b) coleta de dados para trabalho e tabulação por sistemas de monitoração da segurança em informática;

c) atas de reuniões, relatórios de atividades, depoimentos tomados, situações registradas de momentos de insegurança vivenciados em informática;

d) entrevistas, visitas, constatações, análises realizadas e amostras coletadas são, também, formas de atendimento à segurança instalada;

e) treinamento no cumprimento de planos de segurança/de contingência.

Na realidade, o atendimento a situações de insegurança ocorre em momentos simulados, ou, em casos reais, quando qualquer falha, deslize, má prática de medidas de segurança acarretarão danos, normalmente, irreparáveis, em casos de erros, acidentes, falhas, roubo, perda total ou parcial de ativos tangíveis e intangíveis.

O registro da insegurança é vital para futuras análises em termos de caracterização de parâmetros de sensibilidade, definidores de causas, fraquezas, conseqüências, determinantes do evento de insegurança ocorrido.

2.4.1 Segurança sob foco dos usuários

O primeiro elemento principal da segurança do servidor *web* considerado por Evans (1998) é a autenticação da senha e do nome de usuário. Há três aspectos da autenticação de senha e de nome: o nome de usuário, a senha relativa a este nome e o que é permitido a este usuário quando o nome e senha corretos são digitados. Nomes e senhas não têm sentido a menos que se especifique um diretório, uma árvore de diretório ou um nome de arquivo ao qual se aplicam as restrições de acesso ao seu nome/senha.

Quanto à autenticação de nome de usuário e senhas, o autor Evans (1998) ressalta a necessidade em informar a senha e nome apenas uma vez na sessão do *browser*, a menos que as regras de acesso sejam alteradas enquanto se move pelas páginas *web* da intranet. Enquanto o usuário se mantiver nessa sessão, terá acesso a todos os arquivos e diretórios disponíveis para ele segundo as regras de acesso mais recentes, sem precisar digitar novamente seu nome e senha. É conveniente para clientes não precisar informar seus nomes e senhas a cada etapa do caminho desde que as regras de acesso permaneçam inalteradas.

Adicionalmente, cabe lembrar que os usuários têm maiores responsabilidades com os aspectos de segurança no ambiente de microinformática, em face da maior liberdade de uso e exploração dos recursos nestas plataformas. Neste contexto, considerando o comportamento profissional dos funcionários que atuam com a utilização de microinformática, segundo Gil (1994), é preciso reconhecer essa situação, através dos aspectos a seguir:

a) desqualificar a importância não é o posicionamento adequado e, portanto, os argumentos a seguir devem ser tratados com reservas:
   - nossos sistemas são adequados e seguros;
   - isto não aconteceria conosco;
   - não temos qualquer acesso remoto;
   - é muito caro, não podemos pagar por segurança;
   - as áreas empresariais não querem novos dispositivos de segurança;
   - nossas informações não são confidenciais;
   - nossos funcionários são honestos e idôneos;
   - a alta administração só ficará sensibilizada quando o problema ocorrer;
   - acidentes sempre ocorrem e não há como fugir deles;
   - o mercado e a concorrência não estão interessados em nossas práticas empresariais;
   - pequenos desvios de informações e de processos operacionais são inevitáveis;
   - nossa infra-estrutura está em condições adequadas para a manutenção da operacionalidade empresarial;

b) há necessidade de informações seguras como resultado de:
   - crescente utilização de computadores e de suas redes, no suporte às operações empresariais;
   - necessidade da apuração de responsabilidades, quando da guarda e gerenciamento das informações;
   - complexidade e controle e gerenciamento de redes corporativas;

- valor das informações transmitidas de estação para estação, ou arquivadas em bancos de dados corporativos (em nível *mainframe*), de servidores (em nível de servidores de redes), locais (em nível de *work stations*, pessoais (em nível de *desk top* e microcomputadores portáteis;
- das crescentes facilidades de acesso às redes corporativas internas e externas às organizações;
- disseminação da tecnologia de informática pela sociedade;

c) aplicação de tecnologia, em termos preventivos, detectivos e corretivos, que enfrente as seguintes características de violação de segurança:

- exposição, em termos de: revelação não autorizada de dados, modificação de dados ou legítimo acesso negado;
- agressões ao canal de comunicações nos momentos: de interrupção de transmissão de dados por falha e dificuldades com a tecnologia de comunicações;
- interceptação via captação indevida das transações trafegadas;
- modificação em face da adulteração das informações transmitidas no *link* de comunicações;
- fabricação de dados e sua agregação à transmissão vigente no canal de comunicações.

d) falta de sintonia dos dados com o binômio linhas de negócios, sistemas aplicativos, com relação ao:

- sigilo com a manutenção dos dados e programas da organização sob o conhecimento restrito dos profissionais autorizados;
- integridade com a garantia da correção dos dados e a confiabilidade que decisões neles baseadas guardam credibilidade;
- disponibilidade com a certeza de poder alcançar os dados, na medida das necessidades de seu uso.

Um sistema de programação para usuários que está relacionada com a segurança é o *lotus notes*, da IBM. O *Lotus Notes* é um sistema de trabalho que oferece *groupware* para usuários e possui uma imensa base de três milhões de usuários. Além disso, de acordo

com Stewart (1997) uma estimativa de treze mil parceiros comerciais cria suplementos do *notes*, a carga de usuário recomendada para o *note* é de quinhentas a mil pessoas por servidor.

Afirma ainda, que o *notes* é obstinado por segurança e oferece ferramentas de programação que podem incluir formulários; por exemplo, o *lotus script*, que tanto o cliente quanto o servidor podem utilizar. Segundo o autor, os sistemas proprietários como o *notes* podem escolher o padrão de segurança desejado para seu produto e os desenvolvedores do *notes* podem empregar o protocolo de segurança por criptografia de chave pública RSA (o nome se origina de seus criadores: Rivest, Shamir e Adleman). Equipado com o RSA, o *notes* oferece de acordo com Stewart (1997) quatro níveis de segurança:

- Autenticação: a autenticação bidirecional do *notes* exige que servidores e clientes se identifiquem corretamente antes que uma troca de informações comece;
- Controle de acesso: a capacidade de controlar quem acessa o quê;
- Criptografia em nível de campo: documentos podem ser divididos em campos, e seções selecionadas podem ser criptografadas;
- Assinaturas digitais: essas assinaturas servem para assegurar que a informação foi realmente enviada conforme afirmado.

No entanto, a aplicação de sistemas de segurança nas organizações exige também um controle frequente em detrimento da má conduta por parte de seus usuários.

2.4.2 Controle da segurança em informática

O controle é tarefa importante para a qualidade da segurança praticada em informática.

As seguintes atividades são pertinentes, segundo Gil (1994), ao controle da segurança em informática:

a) confronto das causas e conseqüências flagradas/registradas nas situações/momentos de insegurança (ameaça concretizada, por agente agressor, segundo o foco de vulnerabilidade do bem, em determinado perímetro de proteção), em face daquelas estimadas como de ocorrência provável, quando da realização do planejamento;

b) análise do desempenho das medidas de proteção operacionalizadas diante de:
   - padrões de efetividade pretendidos;
   - normas de funcionamento descritas;
   - treinamento, em simulações de insegurança, praticado;
   - intensidade de proteção preventiva, detectiva, corretiva, restauradora alcançada com as ações de segurança concretizadas;

c) realimentação dos processos de planejamento e de execução com a realização das seguintes atividades:
   - apresentação dos desvios ocorridos aos responsáveis por planejamento e por execução da segurança em informática;
   - argumentação quanto á possibilidade de alcance dos padrões estabelecidos e às condicionantes das medições da execução retratadas;
   - proposições de reformatação, reavaliação de padrões com discussão de alternativas, via análise de tolerância (estabelecimento de padrões dentro de faixas de limites, ou seja, definindo um intervalo padrão dentro de faixas de limites, ou seja, definindo um intervalo padrão dentro do qual as medições da execução são consideradas adequadas), com aumento da possibilidade de alcance de desvio zero;
   - explicação de novas formas para que a execução atinja, atenda ao planejamento realizado.

O controle tende a apontar desvios e apresentar proposições a serem consideradas pelo planejamento e pela execução de padrões realizados para que se possa reavaliá-los e melhorá-los.

Em uma organização, de acordo com Caruso (1999) o planejado raramente atende a todas as situações que aparecem e freqüentemente há necessidade de acertar desvios de

rota ou até mesmo mudar o planejado anteriormente. Alega que a fixação de objetivos a serem atendidos, bem como, a definição dos meios e recursos com o estabelecimento de etapas e prazos constituem aspectos da política de segurança (CARUSO, 1999).

Em verdade, o ponto de partida de um projeto eficaz de segurança em informática na organização deve ser a análise dos aspectos que precisam ser cobertos considerando-se os tipos de segurança existentes.

2.4.3 Tipos de segurança

A segurança abrange, segundo Gil (1994), momentos da tecnologia de segurança física/ocupacional/ambiental e da segurança lógica/confidencialidade/organizacional em informática.

2.4.3.1 Segurança física e ocupacional

A operacionalização da segurança física/ocupacional/ambiental em informática é uma tarefa que envolve os profissionais da organização e sua implantação pelo analista de segurança. Sobre este aspecto, Gil (1994) afirma que a segurança física em informática corresponde à manutenção das condições operacionais e da integridade dos recursos materiais componentes dos ambientes e plataformas computacionais como:

a) *hardware* (unidade central de processamento, terminais, impressoras, *disk drive*, monitores);
b) insumos de informática como o formulário contínuo, disquetes, fita de impressora, fitas magnéticas;
c) componentes de informática do tipo *no-break*, cabos de conexão de equipamentos e para transmissão de dados, estabilizadores.

Considerando esses recursos materiais Gil (1994) assinala as seguintes agressões:

a) sabotagem no sentido de tornar inoperante *hardware*, insumos e componentes de informática;
b) terrorismo para avaria de máquinas, equipamentos e insumos;
c) espionagem com o objetivo de captação da estrutura das redes de informática, ou seja, de sua arquitetura e soluções inovadoras, na combinação do trinômio *hardware*, insumos e equipamentos", determinantes de vantagem competitiva na operabilidade de plataformas e sistemas de informática, para atendimento às linhas de negócios empresarias;
d) roubo e furto de recursos materiais, desestabilizando a continuidade operacional e subtraindo patrimônio da organização;
e) acidente causando avaria e paralisação total ou parcial do funcionamento dos aplicativos de informática, por afetar máquinas, equipamentos e dispositivos de processamento eletrônico de dados;
f) explosão com destruição dos recursos materiais computacionais;
g) desabamento com avarias parcial ou total;
h) incêndio espontâneo ou má conservação de instalações com conseqüências prejudiciais à integridade física de recursos materiais;
i) inundação com prejuízos aos equipamentos e insumos de informática.

Neste sentido, Fantinatti (1988) define que o processo de segurança consiste no planejamento de etapas que englobam desde a escolha do local à instalação dos equipamentos, o computador e seus periféricos. Alguns riscos envolvidos nesse processo, segundo o autor são:

a) incêndio;
b) danos de origem externa ou interna;
c) acidente industrial;
d) desastre natural;
e) defeito nas instalações.

Em se tratando do centro de computação, Fantinatti (1988) aponta sua composição pela sala do computador, sala de equipamentos periféricos/auxiliares, depósitos,

manutenção, ou seja, tudo o que diz respeito ao funcionamento do complexo computacional devem ser considerados no projeto de edificação:

a) para efeito publicitário, o computador deve ser instalado em sala amplamente visível através de vitrinas, separadas da rua ou da sala de recepção por paredes, proporcionando visão panorâmica em todos os sentidos;

b) se não fosse a possibilidade de inundações, o subsolo seria local ideal para instalação, porém como pode haver tal ocorrência esta alternativa deve ser descartada; mesmo que se queira instalar tal local, o custo do projeto ficará extremamente alto;

c) se a edificação não for de uso exclusivo do centro de computação, a sala do computador não deve ficar acima, abaixo ou adjacente a local em que haja riscos que possam vir a ser prejudiciais, a não ser que sejam proporcionados meios de proteção adequados, o que virá certamente a encarecer o custo do projeto;

d) a localização em área interna deve ter preferência sobre a delimitada por paredes externas, em contato direto com o exterior da edificação, para evitar possíveis riscos de sabotagem;

e) se não houver outra alternativa e o computador e o depósito de fitas/cartuchos magnéticos tiverem de ser instalados em salas de paredes externas e se estas ficarem adjacentes à edificação suscetível a incêndio, recomenda-se uma das seguintes providências:
   - fechar os vãos das janelas com alvenaria- esta providência é a mais eficiente sob o ponto de vista de proteção;
   - instalar chuveiros externos sobre as janelas;
   - instalar janelas com vidro inestilhaçáveis.

f) o local deve ter uma entrada que possibilite a passagem do maior equipamento existente no mercado;

g) os materiais de construção empregados devem ser os mais resistentes possível, além da qualidade ser de bom padrão;

h) finalmente, a área onde se encontra o computador e as demais áreas sensíveis devem ser acessíveis somente a pessoas que trabalham no local e a outros indivíduos autorizados para tal; o número de pessoas deve ser o mais reduzido possível.

Outras medidas de segurança física estabelecidas por Fantinatti (1988) incluem:

a) Piso elevado: utilização de piso elevado no ambiente como um meio seguro de correr cabos, tanto elétricos como coaxiais, por baixo das diversas unidades, facilitando desta forma qualquer mudança que necessita ser realizada;

b) Uso de sistema de ar condicionado/ventilação: composto de mais de uma unidade, permanecendo uma delas como reserva, já que uma temperatura estável e umidade controlada influenciam no bom funcionamento do equipamento;

c) Instalações elétricas: a rede de instalações elétricas com alimentação dividida em fases e com ligação de aterramento elétrico de todos os componentes metálicos;

d) Depósito de fita, cartucho e disco magnético: local semelhante com um caixa-forte. (http://pt.wikipedia.org/wiki);

e) Proteção contra água: é importante haver ralos de escoamento, calhas eficientes impossibilitando a infiltração da água utilizada neste processo;

f) Prevenção e combate a incêndio: a prevenção de incêndio começa pela estrutura da construção do centro de computação, cuja construção deve ser independente aos demais locais e distantes de fontes de fogo. Desta forma, reunindo-se detecção e combate um importante passo para minimizar as probabilidades de incêndio poderão evitar uma catástrofe;

g) Vigilância e acesso ao centro de computação: como regra básica devem entrar na sala somente as pessoas que tem seu local de trabalho exclusivo no local e que tem autorização de acesso permanente; o restante deve passar pelo processo de entrada/saída que a empresa adotar.

As condições intelectuais, físicas e psicológicas representam preocupação da equipe de profissionais que operacionalizam o trinômio linhas de negócios, sistemas aplicativos, plataformas de informática.

Considerando o exposto, Gil (1994) alega que investimentos em segurança ocupacional são decisivos para o sucesso de qualquer empreendimento, em particular, na busca da qualidade administrativa, técnica e operacional.

2.4.3.2 Segurança ambiental

Segurança ambiental em informática, segundo Gil (1994), comporta forte impacto e passa a ter nível de interação com segurança empresarial à medida que a distribuição dos sistemas aplicativos e das plataformas de informática ganha caráter mais intenso no sentido da descentralização. A segurança ambiental visa a continuidade operacional da infra-estrutura dos ambientes/plataformas/sistemas de informática pode ser estudada, de acordo com Gil (1994) considerando a localização do ambiente de informação, *layout* físico da área de informática, armazenagem externa de meios magnéticos e canal de comunicação de dados.

As medidas de segurança e proteção estendem-se não só a área do computador propriamente dita, mas também aos ambientes adjuntos de um centro de computação.

Quanto a este ambiente, sua edificação e localização, Fantinatti (1988) estabelece os seguintes requisitos:

a) situar-se em rua de fácil acesso, tendo portanto diversas entradas;
b) evitar lugares onde ocorrem grandes aglomerações ou manifestações públicas;
c) dispor de amplo local para estacionamento e meios eficientes para que veículos de recebimento e entrega de material tenham acesso a uma doca de carga/descarga ou que possam acessar o interior da edificação;
d) evitar locais onde possa haver interdição;
e) não deve localizar em local propício a inundações;

f) ter facilidade de instalação de linhas telefônicas, para eventual teleprocessamento;
g) dispor de sistema de abastecimento de força elétrica eficiente e seguro, de preferência através de cabos subterrâneos;
h) evitar local onde exista a falta de abastecimento de água;
i) isolar o prédio de instalações, depósitos etc. que possam apresentar riscos de incêndio, explosão ou algo semelhante;
j) evitar a proximidade de antenas emissoras de microondas, radar, rádio e televisão, devido à possível interferência no funcionamento do computador. Medida importante, porém não vital, pois há bons meios de defesa para este tipo de inconveniente;
k) ser de construção de concreto/alvenaria ou estrutura de aço/alvenaria;
l) instalar o prédio em local isolado do restante da edificação.

2.4.4 Identificação da necessidade de proteção

Para se iniciar o processo de proteção, uma das primeiras providências é a elaboração da norma genérica que deverá conter todas as diretrizes. Estas deverão ser aprovadas pela alta linha administrativa da empresa e todos os funcionários deverão conhecê-las. A identificação da necessidade de se implantar o processo de proteção deve partir da área que administra o controle da informação. Por se tratar de uma ação preventiva o benefício é subjetivo e o custo é considerado alto.

Identificada a necessidade de proteção, tomada de decisão de implantação do programa de proteção e elaborada a norma básica, define-se a classificação dos bens de processamento de dados. O proprietário é o responsável pela adequada classificação, auxiliado pelo analista de desenvolvimento e o usuário principal de aplicação.

A perfeita classificação da informação é essencial, considerando que é o ponto de partida para que não haja riscos de perda do patrimônio. O centro de computação auxilia

na classificação evitando que se proteja em demasia, ou não se proteja a informação (isto ocorre quando não está bem fundamentado o conceito de segurança). O processo de proteção auxilia a identificar registros que exijam medidas protetoras mais restritas. Segundo Fantinatti (1988), há três formas de classificações de segurança:

a) uso externo: com a utilização cada vez maior do computador, tudo na empresa pode e deve ser colocado nele, faturas, ordem de compra, relatórios para o Governo, guia de importação, ou seja, informações que são de "uso externo" à organização.

b) uso interno: são as informações que só devem ser utilizadas dentro da empresa, podendo ser de conhecimento de todo e qualquer funcionário, porém a divulgação externa à organização deverá ser feita mediante aprovação prévia do proprietário.

c) confidencial: engloba informações da mais alta importância para a organização e de propriedades de maior valor, onde a distribuição deve ficar restrita aos funcionários autorizados, e que delas necessitam para desempenhar suas funções na organização. Alguns exemplos desta classificação são:
   - informações que dizem respeito à venda, custo, lucro e outros resultados financeiros da empresa;
   - informações que exibam o produto na sua íntegra, sua estrutura, características ou coisas afins;
   - dados particulares de funcionários;
   - resumo de dados financeiros tais como movimento do caixa, inventário, investimentos, custos de fabricação;
   - informações que definam processos ou critérios utilizados na fabricação de um equipamento;
   - descrição de características de manutenção e desempenho de serviço ou produto;
   - dados que contenham detalhes sobre o uso que a empresa faz de um produto ou dispositivo;
   - detalhes de esquema de produção, vendas.

Microfilmes, cartões, fitas magnéticas, cartuchos, disquetes ou qualquer meio magnético removível devem ter sua classificação para que possa ser protegido adequadamente pelo usuário.

Quanto à segurança, bem como, ao processo de proteção, de acordo com Fantinatti (1988) destacam-se:

a) *software* aplicativo de controle: é o primeiro passo para iniciar tal processo e, neste caso, a contratação de *software* para controle é necessária e deve ser efetivada;
b) *software* básico: devem ser relatórios com identificação de seus proprietários. Por se tratar de rotinas internas, normalmente encontram-se tais pessoas no departamento de processamento de dados da empresa;
c) *software* aplicativo: o mesmo vale para esta categoria, ou seja, devem ser relacionados com identificação de seus proprietários. Estes, pela natureza da atividade, estão fora do departamento de processamento de dados; porém existem aplicações que também estão dentro deste setor da empresa;
d) dados aplicativos: todos os arquivos em meios magnéticos das aplicações devem ter um padrão e a sugestão é de que se use os três primeiros dígitos do primeiro qualificados idênticos á sigla de cada aplicação. Tendo o padrão, deve-se relacionar todos os arquivos aplicativos;
e) arquivos de *software* básico: baseado nos manuais e contatos com os Analistas de Suporte de Sistemas deve-se relacionar e classificar todos os arquivos que fazem parte dos *softwares* básicos existentes no departamento de processamento de dados;
f) arquivos de uso geral: dentro do contexto existem arquivos que pela sua função são acessados de forma indistinta por todos os usuários, quando em produção. Estes também devem ser relacionados e classificados pelo nível de classificação de segurança;
g) biblioteca de meios magnéticos: entenda-se como meio magnético: fita, cartucho, disco, disquete, sendo que um inventário deve ser feito e uma divisão executada entre as tarefas que geram dados que não são usados

oficialmente pela empresa e as tarefas que geram dados e são oficialmente usados pela empresa. Portanto deve ser elaborada uma relação, seus proprietários identificados e estes devem classificá-los;

h) terminais de vídeo: é um inventário físico, porém deve ser tratado dentro do processo de proteção. Uma relação deve ser confeccionada pelo Proprietário e um exame posterior deve ser feito para saber se procedimentos específicos necessitam ser criados para garantir a segurança;

i) aplicação *on-line*: caso a empresa tenha alguma forma de conversação "*on-line*" entre o usuário final e o computador central, uma relação das transações (programas *on line*) e suas classificações devem ser fornecidas pelo respectivo proprietário.

Desta forma, com a utilização desses processos procura-se evitar ameaças e ataques às informações desprotegidas.

Considerando os processos de proteção Fantinatti (1988), registra basicamente dois tipos de proteção: manual e automático (*software* aplicativo).

a) Manual: Envolve rotinas desenvolvidas internamente que necessitam ser colocadas pelo responsável de desenvolvimento do programa ou afim;

b) *Software* aplicativo de controle: É aquele que foi desenvolvido para efetuar tarefas específicas de proteção de informações.

Nestes termos, Gil (1994) delineia as principais características e técnicas de controle em operações e dados de entrada e saída que devem ser incorporadas aos sistemas aplicativos:

a) Em nível de controles em operações e dados de entrada:

- para barrar ameaças como perda de dados, duplicação de dados, dados errados, dados incompletos, omissão de dados, falta de autorização são realizadas validações do tipo:
- léxica: o dado deve satisfazer certas condições;
- sintática: um conjunto de dados deve satisfazer um conjunto de relações entre eles;

- semântica: o dado deve corresponder a certa realidade ou ao que desejamos que represente (correção/fidelidade);
- estrutural: validação léxica e validação sintática.

b) verificação de numeração/sequência:

- testar se a identificação (numeração) da transação já foi processada ou se está na sequência adequada.

c) verificação visual do conteúdo de telas/planilhas/documentos:

- realizado por profissionais diferentes, segundo o conceito de segregação de funções, através da conferência visual, depois, da listagem de todos ou somente daqueles dados de exceção, alimentados ao aplicativo, ou pelo mesmo profissional que está realizando a digitação dos dados, que será o único responsável pela qualidade dos dados submetidos ao aplicativo.

d) verificação de formato de campos de dados:

- testar se o conteúdo dos campos das transações estão preenchidos de forma apropriada, tanto para dados numéricos como para dados alfabéticos.

e) verificação da complementação de campos de dados:

- testar se os campos das transações para as quais não pode haver brancos, foram preenchidos.

f) verificação da data da transação:

- testar se o dia/mês/ano (e horário) da transação são compatíveis com informações cadastrais ou variáveis.

g) verificação de digitação/entrada de dados:

- testar a exatidão dos dados digitados, através da redigitação dos mesmos e comparação contra o arquivo original. Utilizado para campos alfanuméricos e/ou que não permitem verificações/testes de crítica singela do conteúdo do campo, nem permitem consistência do conteúdo do campo contra cadastro.

h) verificação de coerência dos campos das transações:

- testar a coerência entre si do conteúdo de campos que integram uma transação.

i) verificação de transações pendentes por erro na alimentação de dados incompletos:

- testar se há transações aguardando correção por parte do usuário. Implica a criação e acompanhamento do arquivo de transações pendentes aguardando correção.

j) existência de dígito de verificação:

- testar se houve erro de transcrição ou inversão de algarismos em dados numéricos (campo-chave acesso). O dígito de verificação é calculado no momento do processamento – via rotina de cálculo do dígito de verificação componente do programa de crítica – e o resultado obtido é comparado com o dígito informado na transação.

k) verificação de validade de campos:

- testar se os campos das transações são compatíveis com informações cadastrais ou parâmetros constantes de arquivos/bancos de dados em tabelas.

l) verificação de limites de valor:

- testar se o valor da transação está de acordo com faixas/intervalos (limites inferior/superior) previamente estabelecidos.

m) verificação de totais de processamento:

- testar se o total apurado no ciclo de processamento das transações coincide com totais informados/calculados por usuários ou áreas organizacionais de controle. Os totais podem ser de natureza monetária, quantitativa (documentos, transações, registros, linhas).

Cabe salientar que o desenvolvimento dos sistemas aplicativos deve atender às exigências básicas de qualidade e segurança e a manutenção desses sistemas se, mal gerenciada, implica perda da qualidade do sistema.

Em concordância ao exposto é interessante abordar os principais tipos de segurança considerados na informática argumentados nas obras pesquisadas.

2.4.5 Políticas de segurança

Uma política de segurança é um conjunto de regras, leis e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos.

Segundo Soares (1995), um determinado sistema é considerado seguro em relação a uma política de segurança, caso garanta o cumprimento das leis, regras e práticas definidas nessa política.

Uma política segura deve incluir, com detalhes, regras definindo como as informações e recursos da organização devem ser manipulados ao longo de seu ciclo de vida, ou seja, desde o momento que passam a existir no contexto da organização até quando deixam de existir.

Sob este aspecto da segurança Starlin e Novo (1998) afirmam que a garantia da segurança é considerada um dos processos básicos e prioritários para usuários de uma rede corporativa e para os sistemas e aplicativos utilizados através desta.

Segundo o autor, esse processo apóia-se em tecnologias e métodos específicos, com o objetivo de preservar as três propriedades que definem a segurança de uma rede, ou seja, a disponibilidade dos serviços e das informações, a integridade e a confiabilidade.

O acesso à rede Internet permite que tanto o usuário conecte-se ao mundo como o mundo possa acessá-lo, e esse é o principal problema. Quando ocorre um ataque provocado por *hackers*, o curso das atividades organizacionais ficará prejudicado. O tempo que a empresa terá que ficar inativa valerá um investimento para aumentar o nível de segurança dessa rede.

Para quem lida com dados confidenciais, o sistema de segurança contra acessos indevidos é item essencial. Uma política de segurança pode ser implementada com a utilização de vários mecanismos, como os que se analisam em seguida.

Quando as ameaças que pairam sobre a estrutura de uma rede de uma organização parecem ser esmagadoras, deve-se analisá-las para que possa coordenar suas respostas a elas.

Hacker é o indivíduo malicioso e intruso que tenta obter acesso a informações confidenciais através de espionagem.Daí termos *hacker* de senha, *hacker* de rede.

2.5 Ameaças na rede

Ao realizar uma análise sobre o assunto, Bennett (1998) considera os seguintes fatores:

a) ameaça mais provável: observa-se onde se está mais vulnerável, não leva em consideração apenas o acesso à rede. Inclui a ameaça por incêndio, sobretensões de energia, roubo;

b) ameaça mais assustadora: as ameaças assustadoras podem ser por dois motivos. O primeiro é que se o evento ocorrer irá causar muitos danos à empresa. O segundo é perceber que a ameaça pode ser assustadora. Se um vírus penetrar no servidor do banco de dados pode-se perder toda a relação do cliente. Seriam necessárias semanas para reintroduzir as informações a partir de cópias impressas, pois todos os *backups* também estariam contaminados;

c) ameaça mais cara: as ameaças que ocorrem com mais freqüência não causam os maiores danos. A maneira lógica de graduar as ameaças parece ser multiplicar a freqüência da ameaça por seu custo monetário;

d) ameaças emergentes: se a empresa possuir uma *lan* ou *wan* isolada, pode-se pensar que ela está a salvo de ameaças externas. Porém , se tiver acesso à Internet, ou a *wan* pública como espinha-dorsal *(backbone),* já não se pode ter mais certeza.

Considerando estes tipos de ameaças, Bennett (1998) aponta os aspectos a seguir:

a) as redes nunca podem ser totalmente seguras. Quando sela-se a porta lateral, alguns dos mais inteligentes hackers começarão a trabalhar em outra;

b) as informações não podem se manter confidenciais para sempre;

c) novas ameaças continuarão a surgir e podem ultrapassar a estratégia de segurança;

O conceito de segurança pode ser compreendido, porém torna-se necessário estar atualizado quanto a esse aspecto.

A ameaça consiste em uma possível violação da segurança de um sistema e de acordo com Soares, Lemos e Colcher (1995) algumas das principais ameaças às redes de computadores são:

a) destruição de informações ou de outros recursos;
b) modificação ou deturpação da informação;
c) roubo, remoção ou perda de informações ou de outros recursos;
d) revelação de informações;
e) interrupção de serviços.

As ameaças podem ser classificadas, segundo Soares, Lemos e Colcher (1995) como acidentais ou intencionais, podendo ambas serem ativas ou passivas.

As ameaças acidentais são as que não estão associadas à intenção premeditada. A concretização das ameaças intencionais variam desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema. A realização de uma ameaça intencional configura um ataque.

Ameaças passivas são as que, quando realizadas, não resultam em qualquer modificação nas informações contidas em um sistema. Já, uma realização de ameaça ativa a um sistema envolve a alteração da informação contida no sistema, ou modificações em seu estado ou operação.

A materialização de uma ameaça intencional configura em ataque. Assim, na opinião de Soares, Lemos e Colcher (1995), os principais ataques são os seguintes:

a) personificação: uma organização faz-se passar por outra. Uma entidade que possui poucos privilégios pode fingir ser outra, para obter privilégios extras;
b) *replay*: uma mensagem, ou parte dela, é interceptada, e posteriormente transmitida para produzir em efeito não autorizado. Por exemplo, uma mensagem válida, carregando informações que autenticam uma entidade A, pode ser capturada e posteriormente transmitida por uma entidade X tentando autenticar-se no sistema (possivelmente personificando a entidade A);
c) modificação: o conteúdo de uma mensagem é alterado implicando em efeitos não autorizados sem que o sistema consiga detectar a alteração;

d) recusa ou impedimento de serviço: ocorre quando uma entidade não executa sua função apropriadamente ou atua de forma a impedir que outras entidades executem suas funções. Uma entidade pode utilizar essa forma de ataque para suprimir as mensagens;

e) ataques internos: ocorrem quando usuários legítimos comportam-se de modo não autorizado ou não esperado;

f) Armadilhas: ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando (emitido pela entidade que está atacando o sistema) ou a um evento, ou seqüência de eventos pré - determinado;

g) Cavalo de tróia: nesse ataque, uma entidade executa funções não autorizadas, em adição às que está autorizada a executar. Um procedimento de *login* modificado, que, além de sua função normal de iniciar a sessão de trabalho dos usuário, grava suas senhas em um arquivo desprotegido, é um exemplo de cavalo de tróia.

2.5.1 Vírus e outras ameaças

Os vírus são programas hostis que furtivamente obtêm acesso ao computador e freqüentemente tentam destruir ou alterar informações armazenadas no sistema. De acordo com Gil (1994) cada meio usado para transmitir informações eletrônicas pode ser um caminho para um vírus obter acesso à intranet, incluindo produtos comerciais. A ameaça do sistema de computador contrair um vírus segundo o autor é real, mas isso é pouco freqüente e evitável.

Recomenda-se o estabelecimento de uma política de meio externo restrito e a instalação de um software antivírus residente na memória para cada intranet. Se a intranet possui um canal para a Internet ou para outro serviço *on-line*, cada transferência de dados

precisa ser examinada apropriadamente por uma ferramenta antivírus específica do serviço antes de permitir a entrada nos limites eletrônicos da rede.

É importante salientar, porém, que a proteção contra vírus pode perturbar rotinas de trabalho ou ainda causar destruição de bibliotecas de arquivos, de programas ou dados.
Para combatê-los, Cassarro (1997) destaca, portanto, o emprego de vacinas, restrição de acesso a não utilização de programas que são cópias dos originais e utilização de uma política rigorosa de *backup*.

Outras ameaças apontadas pelo autor são bombas-relógio, *worms* e cavalos de tróia cuja a intenção é provocar destruição ou pelos menos caos em sistemas de computador e redes. Os vírus são mais chegados a atos de vandalismo do que roubo ou fraude. Programadores que projetam esses programas geralmente o fazem porque é um desafio e porque é divertido, e eles são normalmente lançados de forma anônima, de modo que o perpetrador realmente nada tem a ganhar a não ser a satisfação de espalhar o caos e a destruição entre sistemas de computador (GIL,1994).

Existem diferenças entre programas destrutivos classificados como vírus, bombas-relógio, worms e cavalos de tróia. Os vírus e worms copiam-se de um sistema a outro, e os cavalos de tróia ficam escondidos dentro de software funcional e são geralmente projetados para simplesmente destruir o sistema no qual residem.
Considerando os riscos ao sistema derivados da intervenção de pessoas no ambiente de processamento de dados de acordo com Gil (1994) são:

a) riscos que afetam a garantia dos serviços:

- negligência ou abandono do serviço por operadores, programadores, usuários, analistas;
- greves, conflitos, paralisações motivadas por divergências entre profissionais ou destes com a organização;
- falta de disponibilidade extra do pessoal em momentos críticos ou de emergência;
- inadequado uso das instalações;
- dependência de sistemas aplicativos dos profissionais que o conceberam/desenvolveram.

b) riscos que afetam a segurança dos dados/informações:

- roubo de informação (ativos intangíveis computacionais);
- manipulação indevida da informação;
- uso indevido (voluntário, ou não) das chaves e códigos de segurança;
- negligência no arquivamento/transmissão de dados/distribuição de informações;
- falta de confidencialidade no tratamento de arquivos e programas;
- fraude, vingança, displicência no tratamento dos recursos integrantes das plataformas de informática.

c) riscos de natureza diversa:

- sabotagem, terrorismo, dano voluntário às intalações;
- intervenção (intrusão, captação) nas linhas de transmissão;
- negligência na observação de normas

Diante dos riscos e ameaças inerentes às informações organizacionais torna-se necessário dispor de mecanismos de proteção.

2.6 Segurança na intranet

As necessidades de segurança numa rede de computadores apresentam-se como uma preocupação que deve ser compartilhada por todos, inclusive o usuário final. Por mais seguro que um sistema operacional seja, as atitudes de um administrador sem treinamento formal ou até mesmo informal podem transformá-lo em uma fortaleza com portas abertas, prontas para receber todo tipo de ataque e invasões.

Diante do exposto, um nível básico de segurança comentado por Stewart (1997) é inerente a todos os sistemas de computador, cujo grau de segurança em um determinado sistema pode variar da restrição total ao acesso público completo.

A maioria das intranets se coloca em algum ponto intermediário, adotando um esquema de círculos concêntricos. Essa estrutura emprega diversos meios para oferecer ou

limitar o acesso e exige que cada nível de segurança seja ultrapassado, de forma semelhante a passagem de um nível de jogo para o seguinte. Assim, as restrições tornam-se maiores à medida que as camadas aprofundam-se, e a obtenção de liberação da segurança para acessar as camadas mais internas pode ser um processo complicado.

As organizações não são rápidas para declarar suas falhas na segurança, de modo que a obtenção de valores exatos sobre a segurança das intranets (além da certeza otimista oferecida por seus fornecedores é um pouco difícil).

Um dos percalços considerados por Stewart (1997) é que nem sempre é possível saber quando houve o acesso ilegal . Embora os hackers mais audaciosos deixem dicas surpresa para mostrar que conseguiram se infiltrar, os hackers sutis podem entrar e sair de uma intranet sem deixar muitos vestígios. Assim à medida que mais e mais informações entram *on-line*, a questão da segurança torna-se muito mais importante . As tecnologias que permitem proteger o armazenamento e o transporte de dados em uma rede consideradas por Benett (1997) são: autenticação, controle de acesso e criptografia.

a) Autenticação: é o processo que consiste em verificar a identidade de um usuário. Muitas redes, inclusive intranets, podem ser configuradas para autenticar o usuário através de um diálogo de solicitação/resposta. De modo geral, esse processo assume a forma da solicitação do nome do usuário e uma senha. Uma autenticação mais rígida pode ser implementada através da tecnologia de chave pública – criptografia. Os servidores http são propensos a alguns problemas específicos de segurança, decorrentes do fato de que as permissões têm de ser abertas o suficiente para permitir que os usuários acessem páginas *web* e executem *scripts cgi*. Determinados processos executados em um servidor por um navegador *web*, por exemplo, podem enviar correspondência eletrônica, remover arquivos e até mesmo formatar disquetes. Os *scripts* representam, portanto, um grande furo de segurança em qualquer *web*, porém existem técnicas bem-documentadas destinadas a eliminar esse furo;
b) Obtenção de acesso: a autenticação resulta em um relacionamento confiável entre o cliente e o servidor. Uma vez que o servidor confie no cliente, ele concederá ou negará acesso a determinados recursos com base em uma tabela

associada a cada recurso, denominada acl (access control list). A maneira como se deve configurar o controle de acesso varia em função do servidor e do sistema operacional de rede utilizados;

c) Criptografia: funciona através da codificação do texto de uma mensagem através de uma chave, que é apenas um número muito longo. E quanto maior a chave, mais rígida é a criptografia . A idéia é de que as chaves rígidas exigem uma capacidade computacional impossível de ser obtida para serem violadas.

Finalmente, para configurar um servidor capaz de proteger a comunicação, precisa-se de um certificado digital. Os certificados atestam que a pessoa que possui uma chave pública é realmente quem alega ser. Nesse sentido, os certificados são a última palavra em autenticação de usuários, e as assinaturas digitais baseadas em chaves privativas oferecem o mais elevado nível de confiabilidade.

2.6.1 Dispositivos de segurança de uma intranet

É possível tomar medidas no servidor *web* para instalar os dispositivos de segurança, aumentar a segurança dos serviços da rede tcp/ip que fazem parte da intranet e dos próprios browsers *web* dos clientes para limitar o que se pode fazer com eles.

Há uma ampla gama de dispositivos de segurança bastante flexíveis que se pode implementar no servidor *web*. Eis alguns relacionados por Evans (1998):

a) Pode-se determinar que o acesso a servidores, páginas individuais ou diretórios inteiros da *web* seja feito mediante um nome de usuário e senha;

b) Pode-se determinar que o acesso a servidores, páginas individuais ou diretórios inteiros da *web* seja limitado a clientes de sistemas específicos. (o acesso será negado a menos que o usuário esteja em sua própria estação de trabalho);

c) É possível organizar indivíduos em grupo e dar acesso a servidores, páginas individuais ou diretórios inteiros da *web* com base no grupo;

d) É possível organizar computadores em grupos e dar acesso a servidores, páginas individuais ou diretórios da *web* com base no grupo;

e) *Scripts* no servidor *web* podem usar quaisquer das restrições de acesso acima, mas é preciso cuidado ao redigi-los para garantir que não ocorram erros relativos á segurança;

f) Alguns programas de servidor http são capazes de se comunicar com browsers *web* de maneira criptografada, cuja segurança é passível de verificação, barrando até os curiosos da rede e garantindo a confidenciabilidade da transmissão de dados pela intranet.

É possível combinar esses dispositivos de várias formas, como requisito de senhas e limite de acesso a um grupo de usuários que precisam acessar o servidor *web* a partir de um grupo específico de sistemas. Ainda, segundo Evans (1998) além do controle de acesso que pode ser instalado no servidor, pode-se garantir a segurança de outros serviços da rede, alguns deles são:

a) o acesso ao servidor ftp anônimo pode ser limitado de várias maneiras importantes, da mesma forma que o servidor http, garantindo ainda assim a transferência de arquivos feita por clientes autorizados;

b) da mesma forma, o acesso ao servidor de notícias *usenet* também pode ser limitado;

c) o acesso a índices e bancos de dados pesquisáveis da intranet pode ser controlado por meio de interfaces *web* protegidas por senhas;

d) o acesso a serviços *gopher* pode ser controlado com base nos endereços de tcp/ip e permissões separadas para pesquisar, ler e buscar podem ser estabelecidas para cada diretório.

Quanto a segurança dos *browsers*, Evans (1998) alega que alguns *browsers web* podem ser configurados de um modo que limitem as características do pacote que os usuários podem acessar.

Os usuários não podem salvar, imprimir ou ver a fonte *html* das páginas *web*, nem mesmo sair do *browser* e reiniciá-lo no modo normal sem sair também do *windows*. Nem

mesmo a janela principal pode ser minimizada ou maximizada, e as caixas de controle de menus suspensos para o *windows* não ficam disponíveis.

2.6.2 Segurança Lógica e a intranet

A modificação acidental ou proposital de recursos tecnológicos/ativos intangíveis, agregados a recursos humanos e materiais é o objeto das práticas de segurança lógica exercitadas na empresa em informática. Considerando o exposto, Gil (1994) assinala os ativos intangíveis:

a) programas de computador integrantes do sistema de aplicativos;
b) software de suporte e básico;
c) procedimentos praticados para atuação com a tecnologia de informática;
d) dados e informação, armazenados em bancos de dados e arquivos, sustentados por dispositivos de computação.

Já para Fantinatti (1988) a segurança lógica em informática manifesta o desafio de desenvolver rotinas capazes de identificar e utilizar técnicas automáticas para preservar de modo adequado as informações de caráter restrito, evitando sua divulgação e modificação não autorizada. Segundo o autor cada organização tem uma necessidade de proteção ou meios para implementar rotinas, não existe solução padronizada e sim diretrizes genéricas (FANTINATTI, 1988). São elas:

a) determinar e identificar de forma clara as responsabilidades de cada função envolvida no processo de proteção. Isto implica montar um organograma eficaz e fazê-lo funcionar dentro das teorias administrativas conhecidas;
b) implementar medidas de segurança física tradicionais e que já demonstraram eficácia, tais como: pessoal de confiança, portas com chave, identificação por cartão magnético;
c) utilizar *softwares* desenvolvidos para tais funções de controle, como proteção por identificação de usuário, uso de senhas, proteção da localidade do

computador (para casos de rede de teleprocessamento), proteção direta em banco de dados etc. Finalmente usar os registros gravados por este *software* para recompor uma "trilha de auditoria" para análise de eventual fraude ou tentativa desta.

O processo de proteção da informação exige uma equipe de funcionários bem treinada e o operador de computador deve ter uma familiaridade muito grande com os equipamentos que manuseia, pois decisões rápidas e certas podem evitar grandes perdas.

Os funcionários envolvidos diretamente com o processamento de dados devem conhecer de forma clara as normas que regem o processo de proteção da organização e não negar ignorância se houver uma tentativa de violação.

No entanto, as falhas no ambiente computacional comprometendo a proteção da informação podem ser provocadas, de acordo com Gil (1994) segundo os focos a seguir:

a) falhas de hardware em virtude de:

- deficiência da proteção a circuitos, chips ou dispositivos (impressora, *hard disk*, teclados, monitores) das plataformas de informática;
- uso de instruções de *firmware* (software gravados em hardware, em nível de fábrica) privilegiadas;
- emanações magnéticas nos links de comunicação ou *work stations*;

b) falhas de *software* em face de:

- erro, deficiência de sistema operacional/*software* de apoio, adquiridos de terceiros;
- má operacionalização de *softwares* aplicativos, de criação própria ou adquiridos de terceiros;
- falhas nos procedimentos de segurança lógica, existentes em normas de contingência empresarial em informática.

c) falhas dos usuários nos momentos:

- deturpação, falsificação, má identificação de arquivos e programas;
- abandono de terminais com dados expostos nas telas;
- tentativas e busca de maneiras de burlar a integridade de informações e sistemas;

- administradores que não assumem suas responsabilidades em termos de segurança;
- displicência de usuários, profissionais de informática, em não cuidar dos relatórios, em função do nível de sensibilidade das informações neles contidas;
- curiosidades, uso indevido por profissionais insatisfeitos, demitidos com ideologias constantes com o foco da organização.

d) falhas de profissionais de informática quando de:

- acesso a software (aplicativos, de suporte, básico) e a arquivos, em nível operacional;
- desenvolvimento de sistemas, programas quebra-galho, que aplicam procedimentos operacionais inadequados, em não-conformidade com normas e metodologias;
- acerto e realização de cópias de arquivos e de programas por meios não autorizados;
- desarme, descumprimento de esquemas de segurança, não entendimento ou não aceitação de práticas de segurança.

Quanto às principais vulnerabilidades, em termos de segurança lógica, podem ser identificadas como:

a) Impedimento de execução de serviço ou descontinuidade operacional;
b) Perda revelação e modificação não autorizada de informações e de software;
c) Uso não autorizado de informação, *softwares*, plataformas de informática;
d) Criação não autorizada de informação e relatórios negociáveis.

Entretanto, a maioria dos incidentes que causam perdas em informática não são de natureza criminosa/intencional, mas ocorre, segundo Gil (1994) por negligência, incompetência, displicência, falta de treinamento de usuários e do pessoal de informática. Profissionalismo, conscientização, treinamento, motivação são fatores importantes para a adequada segurança empresarial em informática.

A atribuição de grau de sigilo e a prática de medidas e mecanismos condizentes à segurança são de responsabilidade conjunta dos proprietários da informação, da área de informática e da administração da organização.

2.7 Proteção das informações

As necessidades de segurança em uma rede de computadores apresentam-se em diversos níveis e aumentam proporcionalmente à heterogeneidade dos sistemas utilizados. Os vários mecanismos de segurança a serem implementados devem interferir o mínimo possível no funcionamento tradicional dos serviços a que os utilizadores estão habituados. Conexões essenciais de rede e fluxos de negócios precisam ser protegidos de ataques externos, exigindo um bom número de ferramentas de segurança e medidas defensivas.

Sobre este aspecto, O´brien (2004) considera a criptografia, *firewalls,* defesas contra negação de serviços como três importantes salvaguardas de segurança. Dentre estas medidas defensivas vale destacar também a utilização de *backups*.

2.7.1 Criptografia

Quanto a criptografia Volpi (2001) conceitua ser responsável pela transformação de dados de maneira a torná-los incompreensíveis sem o conhecimento apropriado para a sua tradução. Segundo tal conceito, Soares, Lemos e Colcher (1995) completam que a criptografia surgiu com a necessidade de enviar informações sensíveis através de meios de comunicação não confiáveis, ou seja, em meios onde é possível garantir que um intruso não irá interceptar o fluxo de dados para leitura (intruso passivo) ou para modificá-lo (intruso ativo).Entende-se o processo de tornar a informação inelegível por encriptar, enquanto descriptar é o processo inverso, ou seja, retornar o código para algo compreensível.

A partir da evolução dos meios de criptografia, podem-se encontrar dois diferentes processos de cifragem (criptografia): a criptografia simétrica (convencional) e a criptografia assimétrica (chave pública).

A criptografia simétrica é o uso de uma chave secreta, a qual o emissor usa para codificar a informação, e , posteriormente, o destinatário utiliza para decifrá-la.

Um dos pontos negativos atribuídos por Albertin (2000) em referência à criptografia com chave secreta são as técnicas de chaves compartilhadas que se deparam com o problema de distribuição de chave, uma vez que as chaves compartilhadas precisam ser seguramente distribuídas para cada par das partes da comunicação. A distribuição segura das chaves torna-se um incômodo nas grandes redes.

Quanto a criptografia assimétrica (com chave pública) Albertini (2000) a caracteriza como uma forma mais forte de criptografia que envolve o uso de chaves públicas. As técnicas de chave pública envolvem um par de chaves , uma chave privada e uma chave pública associadas a cada usuário.

A informação criptografada pela chave privada pode ser descriptografada somente utilizando a chave pública correspondente. A chave privada, usada para criptografar a informação transmitida pelo usuário, é mantida secreta. A chave pública é utilizada para descriptografar no destinatário e não é mantida secreta. Uma vez que somente o autor de uma mensagem criptografada tem conhecimento da chave privada, uma descriptação, com sucesso utilizando a chave pública correspondente verifica a identidade do autor e assegura a integridade da mensagem.

Finalmente, a criptografia com chave pública pode ser utilizada para a autenticação de emissor, conhecida como assinatura digital.

A criptografia de dados de acordo com O'brien (2004), tornou-se uma maneira importante de proteger dados e outros recursos de rede de computadores, principalmente na Internet, Intranets e Extranets. Senhas, mensagens, arquivos e outros dados podem ser transmitidos de forma embaralhada e desembaralhados pelos sistemas de computadores apenas para os usuários autorizados. A criptografia envolve o uso de algoritmos matemáticos especiais, ou chaves para transformar dados digitais em um código embaralhado antes que esses dados sejam transmitidos e para decodificá-los quando forem recebidos.

Para Evans (1998), é possível aumentar ainda mais a segurança da intranet criptografando as transações *web*. Quando se usa um dispositivo de criptografia, as

informações dadas pelos usuários nos formulários preenchidos na *web*, incluindo nomes de usuário, senhas e outros dados confidenciais, podem ser transmitidas com segurança de e para o servidor *web*.

O autor afirma que há uma ampla gama de soluções propostas e/ou parcialmente implementadas de criptografia para a *web*, mas a maioria ainda não está pronta para funcionar de maneira completa. Dos vários métodos propostos, somente dois se apresentaram em uma forma próxima da final. Dentre eles existem os seguintes protocolos:

a) S-http: o Secure http foi desenvolvido foi desenvolvido pela *Enterprise Integration Technologies* e RSA Data *Security*, e os padrões públicos S-http agora são gerenciados pela *CommerceNet*, um consórcio sem fins lucrativos que está conduzindo o primeiro teste de mercado em larga escala de tecnologias e processos para permitir o comércio eletrônico via Internet. O S-http é uma versão modificada do protocolo httpd atual. Ele aceita:

- Autenticações de usuário e servidor *web* por meio de assinaturas digitais e chaves de assinatura usando os algoritmos RSA e MD5;
- Privacidade de transações, usando diversos métodos diferentes de criptografia com base em chaves;
- Geração de certificados de chave para autenticação pelos servidores.

b) SSL: o protocolo S-http foi desenvolvido pela *Netscape Communications Corporation*. Em vez de desenvolver um protocolo completamente novo para substituir o httpd o *Secure Socket Layer* (SSL – Camada de Soquete Segura) fica entre o httpd e os protocolos de rede TCP/IP subjacentes e pode intervir para criar transações seguras.

Ainda, vale lembrar que os dois não são compatíveis entre si, apesar de ser possível uma compatibilidade. Browsers *web* e servidores que permitem o uso de um desses métodos não permitem o outro, portanto é possível usar um ou outro de maneira confiável somente se houver uma combinação cuidadosa do servidor *web* com os browsers dos clientes (EVANS, 1998).

2.7.2 *Firewalls*

O *firewall*, segundo O'brien (2004), é um método importante para controle e segurança na Internet e outras redes. Um *firewall* de rede pode ser um processador de comunicações, normalmente um roteador ou um servidor exclusivo operando com software *firewall*. Atua como um sistema de computador guardião, que protege as intranets e outras redes de computadores da empresa contra a invasão, funcionando como um filtro e ponto seguro de transferência para acesso à Internet e outras redes. É capaz de filtrar todo o tráfego de rede em busca de senhas corretas ou outros códigos de segurança e somente permite transmissões autorizadas para dentro e para fora da rede. O autor destaca que *firewalls* conseguem deter, mas não evitar inteiramente o acesso não autorizado (*backing*) às redes de computadores (O'BRIEN,2004).

Diante do exposto, Soares, Lemos e Colcher (1995) considera um *firewall* como uma coleção de componentes, colocada entre duas redes, que possua as seguintes propriedades:

a) Todo o tráfego de dentro para fora da rede, e vice-versa, passa pelo *firewall;*

b) Só o tráfego autorizado pela política de segurança pode atravessar o *firewall;*

c) O *firewall* deve ser à prova de violações.

Um *firewall* pode ser visto como um monitor de referência para uma rede, sendo seu objetivo garantir a integridade dos recursos ligados a ela. Assim, enquanto as máquinas de uso geral são configuradas para otimizar o desempenho e a facilidade de utilização, no *firewall* tudo isso passa para o segundo plano, cedendo lugar ao seu objetivo principal no sistema: a segurança.

Analisando a importância do *firewall,* Evans (1998) adverte sobre a proteção da intranet, bem como a todos os demais bens da rede da empresa. Além disso, a menos que a rede corporativa não se conecte de maneira alguma com o mundo exterior, é provável que se queira garantir a segurança de outros serviços da intranet, incluindo não apenas os servidores *web*, mas também o ftp, gopher, usenet news, wais e outros serviços de rede tcp/ip.

Já para Stewart (1997), os firewalls atuam como bloqueios herméticos que impedem a entrada de algo indesejado. No entanto, a proteção nem sempre é possível quando *hackers* (invasores de sistemas) atravessam a Internet. Já que, de acordo com Stewart (1997), um firewall opera com a seguinte filosofia de segurança: o que não é expressamente permitido é negado. Essa orientação impede que qualquer usuário questionável entre ilegalmente em uma intranet ou que um usuário interno saia dela. Com um firewall, as capacidades de registro de atividade são melhoradas e serviços como autenticação, redes privadas virtuais e tradução de endereços da rede são constantemente utilizados. Neste sentido, como as intranets usam tecnologias *web* e Internet, até mesmo o firewall de mais alta qualidade não pode restringir totalmente o fluxo de informações pra dentro e para fora de uma empresa. Há tantas formas de comunicação eletrônica usadas em uma intranet que torna difícil ou até impossível, monitorá-las completamente. Registrar cada indicador, cada transmissão de correio eletrônico e cada remessa de grupo de discussão de um único usuário da intranet seria um procedimento dispendioso.

Os *firewalls* são classificados, de acordo com Soares, Lemos e Colcher (1995), em três categorias principais: filtros de pacotes, *gateways* de circuitos e *gateways* de aplicação.

a) Filtros de pacotes: utilizam endereços ip de origem e de destino, e portas udp e tcp para tomar decisões de controle de acesso. O administrador elabora uma lista de máquinas e serviços que estão autorizados a transmitir datagramas nos possíveis sentidos de transmissão (entrando na rede interna, saindo na rede interna ou ambos), que é então usada para filtrar os datagramas ip que tentam atravessar o *firewall;*

b) *Gateway* de circuitos: atua como intermediário de conexões tcp, funcionando como um *proxy* tcp (um tcp modificado). Para transmitir dados através do *firewall*, o usuário origem conecta-se a uma porta tcp no *gateway*, que por sua vez, conecta-se usando outra conexão tcp, ao usuário destino. Um circuito é formado por uma conexão tcp na rede interna e outra na rede externa, associadas pelo *gateway* de circuito;

c) *Gateway* de aplicação: ao invés de basear-se em um mecanismo de propósito geral como os filtros de pacotes, utilizam implementações especiais de aplicações desenvolvidas especificamente para funcionar de forma segura. Devido a grande flexibilidade dessa abordagem, ela é a que pode fornecer o maior grau de proteção.

Diante do exposto, verifica-se que apesar das empresas fazerem uso de *firewall* para proteger as suas redes, a proteção que elas oferecem nem sempre é suficiente. As ferramentas criadas por intrusos estão constantemente crescendo em sofisticação e velocidade, e podem ser automatizadas para criar chances de penetração.

É importante ficar atento a novos aspectos de segurança, pois as falhas na segurança geralmente podem ser sanadas antes de causarem danos maiores. A manutenção cuidadosa do site, assim como a atenção à atividade do site, ajuda a proteger contra problemas de segurança.

Neste sentido, Benett (1997) define *firewall* como um dispositivo que fornece segurança ao acesso e à comunicação entre uma rede privativa confiável, como na intranet, e redes públicas não confiáveis como Internet. Os *firewalls* podem também funcionar como mediadores entre grupos de trabalho dentro de uma empresa. Esse recurso pode ser útil em uma empresa que tenha subsidiárias regulamentadas e não-regulamentadas que compartilhem determinados recursos.

Como um *firewall* fica pelo menos parcialmente visível ao público ele pode funcionar como o portão de entrada da empresa – um local em que informações sobre os seus produtos e serviços ficam disponíveis ao público, em geral funcionando também como servidores *web*. Os produtos de *firewall* podem prestar, com uma margem significativa de segurança, muitos serviços Internet, inclusive *http, ftp, dns e smtp* (correio eletrônico). Cada serviço oferecido dessa forma é chamado *proxy*.

Tecnicamente, *proxy* é um programa que reside no *firewall* e tem acesso aos dois lados da interface – a intranet e a Internet (BENETT,1997) . As solicitações de serviços externos feitas a partir da empresa, como, por exemplo, um navegador *web* que aponte para um *url* remoto, são capturadas pelo *proxy* de serviço http e, se as normas do *firewall* permitirem, são transmitidas para a Internet.

Por outro lado, o tráfego da Internet para a empresa, como por exemplo, correspondência eletrônica, é capturado pelo *proxy* de serviço *smtp* e se as normas do *firewall* permitirem, é transmitido para a intranet.

Outra vantagem dos servidores *firewall/proxy* consiste no fato de que todos os serviços acessados através do *firewall* são registrados no *log* do sistema (se o servidor estiver configurado para essa finalidade), o que fornece uma trilha interna de auditoria referente às transações realizadas com o mundo externo.

2.7.3 Defesas contra negação de serviço

Os procedimentos básicos que as empresas de *e-business* e outras organizações podem adotar quanto à negação dos serviços, consideradas por O'brien (2004), são:

a) nas máquinas **zumbis**: estabelecer políticas de segurança. Procurar constantemente programas cavalo de tróia e pontos vulneráveis. Fechar portas não utilizadas. Pedir aos usuários para não abrir arquivos *.exe* anexados à correspondência;
b) no ISP: acompanhar e bloquear obstruções ao tráfego.Filtrar endereços IP sem sentido. Coordenar a segurança com provedores de rede;
c) no *website* da vítima: criar servidores de reserva e conexões para cada servidor. Instalar sistemas múltiplos de detecção de invasões e roteadores múltiplos para o tráfego de entrada para reduzir os pontos de choque.

2.7.4 *Backup*

A realização de *backups* regulares de acordo com Stewart (1997) é uma maneira de garantir que os dados sejam protegidos. Todos os dados armazenados em um servidor

estão sujeitos a vírus, alterações, exclusões e até troca de lugar. Os *backups* garantem que os dados da organização dos trabalhos estejam seguros, porém são inúteis se não forem atualizados e armazenados em um local seguro e facilmente acessáveis.

A criação de novos dados em uma intranet diariamente implica a realização de *backups* desses dados todos os dias. Segundo Stewart (1997) cada utilização da intranet equivale a oitenta e seis mil e quatrocentos segundos em que um usuário, um *bug* de *software*, um vírus, uma falta de energia tem a oportunidade de destruir os dados.

Mesmo que se realizem *backups* diários, mantê-los no mesmo local da intranet é quase tão ruim quanto não fazê-lo. Há muitos desastres naturais e humanos que podem destruir a intranet e os *backups* em uma ação rápida – enchente, furacão, incêndio, submersão e até mesmo explosões. Ter discos de *backup* imediatamente em mãos pode ser conveniente, mas não é seguro. Segundo Stewart (1997) é interessante transportar regularmente os discos de *backup* para uma instalação de armazenamento em local diferente. A maioria dos pacotes de *software* de *backup* opera apenas dentro de um sistema operacional específico, porventura poderá ocorrer ao restaurar cada arquivo em uma máquina erros ou outras dificuldades, especialmente nas áreas de arquivos de sistema, configuração e segurança.

A realização de *backups* apenas de dados torna-os mais rápidos e mais fáceis de mantê-los. Os dados incluem não só os arquivos criados com um processador de texto mas também correio eletrônico, grupos de discussão, páginas *web*, arquivos gráficos, apresentações de multimídia e dados de agenda. Qualquer bit de informação que não foi colocado na intranet diretamente por meio de um *software* deve ser incluído em um *backup* só de dados. Se essa informação não existe nos *cd-roms* ou disquetes da instalação original, acabará se perdendo caso haja falha na intranet.

Outras medidas de proteção adequadas a ambientes de comunicação de dados merecem ser melhor expostos e estão relacionados a seguir.

2.7.5 Outros mecanismos de proteção

a) Assinatura digital : ao se tratar do tema assinatura digital acaba-se fazendo relação direta aos algoritmos de autenticação. Quanto a este aspecto, Volpi (2001) conceitua algoritmos de autenticação àqueles que operam como elementos de verificação da autoria e do conteúdo dos dados enviados. Eles não trabalham como tradutores de mensagens, sua função é estritamente verificar que aquilo que partiu da origem confere com o que chegou no destino final;
b) Utilização de senhas: muitos administradores de sistema insistem em senhas longas e insistem até mesmo em gerar senhas de modo central e distribuí-las para os usuários em correspondência segura;

Diante do exposto, Bennett (1997) enfoca alguns aspectos a considerar ao elaborar a senha:

a) Quanto mais longa a senha, mais difícil será determiná-la por meio de força bruta. O termo força bruta refere-se ao método que tenta uma série de senhas para nome de usuário até que lhe seja dado acesso ao sistema;
b) Se a senha puder ser escolhida a partir de um conjunto de caracteres maior, a abordagem da força bruta também será mais difícil;
c) Se a senha muda regularmente, então o problema da descoberta física torna-se menos importante;
d) Se a senha for escolhida por um utilitário aleatório, então a força bruta pode ser inútil.

Considerando os mecanismos de controle de acesso, Soares, Lemos e Colcher (1995) afirmam que eles são usados para garantir que o acesso a um recurso seja limitado aos usuários devidamente autorizados. Segundo os autores as técnicas adotadas envolvem a utilização de listas ou matrizes de controle de acesso, que associam recursos a usuários autorizados, ou *passwords* e *tokens* associadas aos recursos, cuja posse determina os direitos de acesso do usuário que as possui.

Considerando o contexto, Caruso (1999) argumenta que os métodos de controle de acesso mais recentes tendem a usar senhas como mecanismo de autenticação de identidade de usuários pela atribuição de uma senha exclusiva ou identificação de usuários individuais. Afirma o autor, à medida que evoluem os equipamentos de leitura e autenticação, há uma forte tendência para que as senhas, constituídas por uma combinação de letras ou números, sejam substituídas por alguma característica física do usuário, como a imagem da íris, a impressão digital ou pela voz.

c) Integridade de dados: para garantir a integridade dos dados podem ser usadas as técnicas de detecção de modificações, normalmente associadas com a detecção de erros em bits, em blocos ou erros de seqüência e redes de comunicação. Caso os cabeçalhos e fechos carregando as informações de controle não forem protegidas contra modificações, um intruso, que conheça as técnicas, pode contornar a verificação. De acordo com Soares, Lemos e Colcher (1995), para garantir a integridade é necessário manter confidenciais e íntegras as informações de controle usada na detecção de modificações;

d) Enchimento de tráfego: O enchimento das unidades de dados fazendo com que elas apresentem um comprimento constante são formas para fornecer proteção contra a análise do tráfego;

Segundo Soares, Lemos e Colcher (1995) o mecanismo de enchimento de tráfego só tem sentido caso as unidades de dados (ou pelo menos os campos de controle) sejam criptografados, impedindo que o tráfego espúrio seja distinguido do tráfego real;

e) Controle do roteamento: para garantir que os dados possam ser transmitidos em rotas fisicamente seguras há possibilidade de controlar o roteamento especificando rotas preferenciais (ou obrigatórias) para a transferência de dados (SOARES; LEMOS; COLCHER, 1995).

f) Segurança física e de pessoal: medidas que garantam a integridade física dos recursos de um sistema são indispensáveis para garantir segurança do sistema como um todo. A segurança de qualquer sistema depende, segundo Soares, Lemos e Colcher (1995), da segurança física de seus recursos e do grau de confiança de pessoal que opera o sistema. Afinal, não se podem utilizar

mecanismos sofisticados de segurança se os intrusos puderem acessar fisicamente os recursos do sistema;

g) *Hardware/Software* de confiança: para que se possa confiar nos mecanismos do sistema que implementam a política de segurança deve-se exigir: a aplicação de métodos de prova, verificação e validação, detecção e o registro das tentativas de ataques identificadas, e adicionalmente, que a entidade tenha sido construída por pessoal de confiança em um ambiente seguro;

h) Rótulos de segurança: rótulos de segurança explícitos devem, como afirma Soares, Lemos e Colcher (1995), ser facilmente identificáveis para garantir que eles possam ser apropriadamente verificados. É importante, também garantir que o escopo do rótulo de segurança permaneça limitado ao recurso ao qual ele está associado. Ainda, o rótulo de segurança deve ser mantido junto com os dados quando eles são transportados;

i) Detecção e informe de eventos: a detecção de eventos relevantes no contexto da segurança inclui a detecção de aparentes violações à segurança e deve incluir, adicionalmente a detecção de eventos normais, como um acesso bem-sucedido ao sistema *(login)*. A detecção de um evento do ponto de vista da segurança, pode, por exemplo, provocar uma das seguintes ações: informe local ou remoto do evento, registro do evento em um arquivo ou a execução de uma ação de recuperação (SOARES; LEMOS; COLCHER, 1995).

Estas são algumas políticas de monitoramento, sendo importante ressaltar que a Internet e outros sistemas *on-line* de *e-mail* são alvos favoritos dos hackers que querem espalhar vírus ou invadir computadores interligados em rede. O *e-mail* também faz parte do campo de batalha para tentativas adotadas pelas empresas para reforçarem as políticas contra mensagens ilegais.

Por outro lado, as verificações e os cálculos através dos quais as informações são mantidas em segurança apresentam custos associados. As senhas devem ser administradas, alteradas regularmente e reatribuídas quando esquecidas. Os *logs* do sistema deverão ser analisados periodicamente para que seja verificada a existência de indícios de acesso não-autorizado. O controle de acesso é tratado em muitos servidores *web* de maneira diferente

do tratamento adotado nos servidores de arquivos e nos *hosts* de uma empresa, o que aumenta de forma significativa o *overhead* administrativo e o risco de erros. A criptografia segura exige certificados digitais, que implicam custos comerciais e administrativos.

Para elaborar um plano criterioso de segurança deve-se considerar os ativos que se pretende colocar à disposição dos usuários através de *webs* internas. Isso abrange os dados, documentos, imagens e recursos de rede a que as pessoas terão acesso. Em seguida deve-se avaliar a vulnerabilidade de cada um desses ativos em relação aos seguintes riscos considerados por Benett (1997):

a) exposição de material confidencial a pessoas não-autorizadas: essas pessoas podem abranger funcionários que não precisem ter acesso a essas informações, profissionais contratados por tempo limitado que tenham privilégios de *login* na intranet ou qualquer outra pessoa, caso a intranet esteja conectada à Internet;
b) danos ou remoção do ativo: esse risco existe sempre que vários usuários têm a capacidade de atualizar informações compartilhadas;
c) uso ilegítimo ou inadequado de recursos compartilhados: esses recursos abrangem arquivos e aplicativos, além de periféricos da rede, como impressoras, digitalizadores *(scanners)*, unidades de *cd-rom* e *modems*.

A segurança praticada nas organizações depende, diretamente da cultura, formal e informal, vigente. Desta forma, normas existentes procedimentos e práticas administrativas cumpridas pelos profissionais da organização, segundo Gil (1994) são determinantes para o nível da segurança empresarial em informática.

3 METODOLOGIA

A metodologia está relacionada com o modo pelo qual uma pesquisa é conduzida. Assim, seguindo a classificação de Mattar (1999), define-se a pesquisa:

3.1 Caracterização da pesquisa

A caracterização da pesquisa permite identificar a natureza das variáveis pesquisadas, podendo ser uma pesquisa qualitativa ou quantitativa. Assim, a pesquisa qualitativa, opção deste trabalho, é concretizada entrevistando-se duas pessoas da área de informática, responsáveis pelo implantação de sistemas de segurança do Tribunal Regional do Trabalho/SC com o auxílio de um gravador. Lembrando que na pesquisa qualitativa, de acordo com Mattar (1999), os dados podem ser colhidos por meio de perguntas abertas (quando em questionários), entrevistas em grupos, entrevistas individuais em profundidade e testes projetivos. Já na quantitativa os dados são colhidos de um grande número de respondentes, usando-se escalas e são submetidos a análises estatísticas.

Quanto à perspectiva do estudo, tem-se a transversal, já que a coleta de dados primários restringiu-se ao período de 02/05/2005 até 23/05/2005 (BABBIE, 1998). Dados primários são àqueles que, segundo Mattar (1999), não foram coletados anteriormente, estando em posse dos pesquisados, e são coletados com o propósito de atender às necessidades específicas da pesquisa em andamento.

3.2 Delineamento da pesquisa

Segundo Mattar (1999), a pesquisa também pode ser classificada quanto aos fins e quanto aos meios. Neste contexto, define-se o delineamento para a presente pesquisa, como segue.

3.2.1 Quanto aos fins

Natureza do relacionamento entre as variáveis estudadas: classifica-se como descritiva, pois considerando a classificação de Mattar (1999), a pesquisa tem por objetivo expor o fenômeno em estudo, ou seja, relaciona-se ao uso da intranet e seus aspectos de segurança, no TRT/SC.

Apresenta caráter exploratório, pois se busca a familiarização e aprofundamento no processo de investigação.

3.2.2 Quanto aos meios

A pesquisa realizou-se em ambiente real (o TRT/SC), ou seja, numa situação real onde procurou-se identificar o relacionamento (causa e efeito) entre as variáveis do fenômeno em estudo, portanto, classifica-se como pesquisa de campo, conforme Vergara (1997).

3.3 Técnica de coleta de dados

Em função do tipo de pesquisa escolhido e da fonte de dados, seguindo a classificação de Mattar (1999), quanto ao levantamento em fontes secundárias caracteriza-se:

a) levantamentos bibliográficos: envolve procura em livros sobre o assunto, revistas especializadas ou não, dissertações e teses apresentadas em universidades e informações publicadas por jornais, órgãos governamentais, sindicatos, associações de classe e concessionários de serviços públicos;

b) levantamentos documentais: às vezes a própria empresa mantém em seus arquivos valiosas informações sobre resultados de pesquisas anteriores, registros de gastos em propaganda e promoção de vendas, número de vendedores por mês e por região, dados sobre produção, estoques e vendas mensais e práticas de preço.

Sendo assim, os meios para a obtenção de dados através de levantamentos bibliográficos e documentais em fontes secundárias foram orientados principalmente pelas obras de Gil, Fantinatti e Stewart.

A coleta de dados primários foi obtida por meio de documentos e entrevistas semi-estruturadas (ver roteiro em apêndice A) realizadas a partir de questões previamente formuladas. Já a coleta de dados secundários efetivou-se basicamente através de livros e da Internet, conforme se observa na lista de referências.

A população pesquisada é composta por 36 funcionários que integram o setor de informática do TRT. Já quanto à amostra, escolhida por acessibilidade (VERGARA, 1997), esta é composta por dois respondentes: George Alexandre Silva (Assistente-Chefe do setor de Administração de Sistemas Operacionais) e Sandro Beltrame (Diretor da Área de Suporte aos Recursos de Informática.

3.4 Limitações (técnicas e estatísticas)

Foi considerado como principal fator limitante para a realização da pesquisa: o tempo para a sua consecução. Os dados obtidos foram consolidados com a utilização de um gravador e simultaneamente por meio de caneta e papel. As informações foram respondidas conforme roteiro em apêndice.

4 APRESENTAÇÃO E ANÁLISE DOS DADOS

A seguir serão apresentadas informações sobre o estudo de caso baseado no Tribunal Regional do Trabalho (TRT).

Pretende-se com este estudo estabelecer uma comparação entre a teoria fundamentada por diferentes autores com a prática na organização em questão.

4.1 Conteúdo e análise do uso da intranet pelos usuários do TRT

A intranet de uma organização utiliza tecnologias da Internet dentro da própria organização. Dentre as tecnologias para a manipulação das informações no TRT faz-se pela conexão de páginas *html*, asp e java ao banco de dados por intermédio do protocolo tcp/ip. Segundo Evans (1998), este é o protocolo central da Internet pelo qual cada computador deve implementá-lo para comunicar-se na rede.

Nestes termos, Starlin e Novo (1998) afirmam que, sendo a intranet uma rede que utiliza as tecnologias da Internet no formato *html* (*web)*, padrão de correio eletrônico smtp, sistema de troca de arquivos pelo ftp, todos esses serviços são executados em conjunto com o protocolo tcp/ip.

Quanto à tecnologia de correio eletrônico utilizada pelos usuários do Tribunal Regional do Trabalho de Santa Catarina, tem-se o *exchange* e *outlook* da *microsoft.* Todavia, segundo Sandro Beltrame, Diretor da Área de Suporte aos Recursos de Informática do TRT/SC, há uma tendência no serviço público em migrar de sistemas pagos para sistemas *free* ou também chamado código aberto como: *e-mail* e servidores de arquivo.

Atualmente o TRT dispõe do *exchange* e *outlook* para serviços de correio eletrônico, no entanto há uma propensão quanto à exclusão do *exchange* para aderir somente ao q-mail, programa servidor de correio eletrônico considerado um sistema *free*.

O correio eletrônico, para Benett (1997), é a mais simples das técnicas de envio/recebimento de mensagens e uma das mais eficientes e duradouras. Parte das vantagens do sistema está na capacidade de entrar em contato com qualquer pessoa da rede, permitindo que sejam enviadas mensagens com arquivos anexados de várias maneiras.

Deste modo, Stewart (1997) também considera o correio eletrônico um bom método para regular o uso da intranet por meio de uma política que defina os limites de sua utilização pelo usuário. Esta situação é evidente no TRT, pois os colaboradores limitam-se a esta tecnologia no que se refere à capacidade de espaço de armazenamento das mensagens. Ao Diretor é disponibilizado maior capacidade e utilização do correio eletrônico quando comparado ao colaborador aquém da sua posição hierárquica. Ao iniciar o projeto de uma intranet, o primeiro passo, de acordo com Stewart (1997), é definir o público-alvo ou clientes. Os clientes são as pessoas da própria empresa, que tornam disponíveis produtos ou serviços. A partir da definição do público-alvo pode-se projetar a intranet e saber quais informações ela conterá. No caso do TRT, todos os funcionários têm acesso à intranet, incluindo advogados e diretores.

Considerando o exposto, a responsabilidade pela gestão de dados no Tribunal Regional do Trabalho/SC é da área de informática. Os técnicos de informática organizam e estruturam o formato geral do banco de dados, porém quem gera as informações que alimentam o banco são os usuários. O Diretor da área de informática, juntamente com os colaboradores da área técnica, desenvolvem ferramentas para que os usuários armazenem informações diretamente no sistema.

Alguns dos serviços que o TRT oferece aos seus usuários encontram-se relacionados a seguir:

a) Sup (Sistema Único de Protocolo): mecanismo utilizado para consultar todos os documentos que estão no Tribunal;
b) Manual de Sistema FGTS: muito utilizado pelos usuários das Varas de trabalho para recolhimento do fundo de garantia por tempo de serviço;

c) Termo provisório: relaciona todos os termos de material permanente, ou seja, a mesa, o computador, a cadeira, todos os materiais que estão sendo utilizados por cada colaborador;

d) Estrutura funcional: permite a consulta do colaborador ao quadro histórico que engloba: número dos documentos de identificação (identidade, cpf), cursos realizados até o momento;

e) Relação de funcionários: permite a consulta do usuário à lotação de todas as pessoas que trabalham no TRT.

Além do acesso a estes serviços os usuários utilizam a intranet para capturar informações sobre Varas do Trabalho, estrutura funcional, consulta à contra-cheques, alterações de senhas, organogramas, cálculos trabalhistas, catálogo telefônico, chamada de suporte, consulta à processos, bens da unidade e bens materiais.

É importante salientar que os serviços e recursos utilizados da intranet são acessíveis a todos os colaboradores, ou seja, todos têm acesso desde que haja a autenticação pelo sistema conforme usuário e senha registrados. As consultas referentes às situações particulares, como a contra-cheques, restringem-se ao próprio usuário, não dispondo deste recurso para consulta de outrem.

Diante das informações disponibilizadas numa intranet, algumas das fontes de recursos citadas por Stewart (1997) é o uso do *help desk*. Quanto a este item, a organização estudada dispõe de um recurso semelhante chamado Sajud – Sistema de chamada de suporte para usuários, portanto possibilita solucionar questões relacionadas a *software* e *hardware*.

A intranet (*home page* em anexo B) é reconhecida como importante fonte de dados e informações para os usuários do TRT (organograma conforme anexo A). Praticamente todos os usuários do Tribunal possuem computador disponível para a realização de suas funções.

Além disso, a intranet fornece uma variedade de vantagens aos seus usuários acelerando a comunicação e a troca de informações.

Algumas dessas vantagens foram apontadas por Sandro Beltrame, e que vêm confirmar os benefícios da intranet relacionados por Stewart (1997) e Albertin (2000)

envolvendo: a facilidade na comunicação interna, variedade de serviços oferecidos aos clientes internos (serviços de pedido de material, controle de patrimônio, correios e outros serviços que só dizem respeito ao Tribunal) e ainda, a facilidade na publicação da informação. A Administração do TRT pode se reportar ao colaborador por duas alternativas: ou por e-mails ou publicação da informação na intranet.

As intranets podem ser beneficiadas com avanços, desenvolvimentos ou melhorias em quaisquer produtos que operem pelo protocolo tcp/ip. As redes padrão comumente limitam-se pelo método de gerenciamento de informações e comunicações semelhante ao *lotus notes*.

Quanto a esta ferramenta, pode-se afirmar que algumas áreas do TRT utilizam o *ms exchange,* porém este sistema não comporta todas as funcionalidades do *lotus notes*.

Por outro lado, vale destacar que a intranet, em virtude da sua utilização em protocolo tcp/ip pode apresentar desvantagens. Uma desvantagem significativa relatada por Stewart (1997) pela utilização do protocolo tcp/ip é a maior demanda na potência geral do sistema e a RAM necessária a cada dispositivo da intranet. Porém, na opinião do Diretor da Área de Suporte aos Recursos de Informática do TRT/SC, a intranet não relaciona desvantagens, sendo considerada uma ferramenta muito boa para comunicação de difusão de informações.

Tanto a importância das informações para as empresas bem como, a tecnologia disponibilizada para armazená-las e acessá-las vêm provocando concomitantemente restrições de acesso aos sistemas. O principal motivo que propicia um controle maior das informações se faz pela ocorrência freqüente de ataques e invasões a serem solucionados pelo setor de informática.

Neste contexto, alguns dos sistemas de segurança relacionados à intranet do TRT são identificados a seguir.

4.2 Identificação dos sistemas de segurança relacionado à intranet do TRT

À medida que o ambiente organizacional aumenta de tamanho e complexidade, aumenta a vantagem e a necessidade da implantação de segurança e controle na rede. Não há uma ferramenta de segurança única, diversos tipos de medidas e ferramentas para obter a segurança são utilizados simultaneamente.

As tecnologias que permitem proteger o armazenamento e o transporte de dados em uma rede considerados por Benett (1997) e que são úteis à organização em questão são: autenticação, controle de acesso e criptografia.

Considerando o exposto, constatou-se que o TRT apresenta sistemas específicos eficazes que protegem as informações contra a maioria dos riscos. Os sistemas de segurança utilizados pelo TRT abordados na entrevista e que condizem com os autores Cassaro (1997) e Stewart (1997) relacionados à segurança lógica são: controle de acesso (usuário/senha), *backups* frequentes, *firewalls*, *gateways*.

A autenticação é o processo que consiste em verificar a identidade de um usuário, esse processo assume a forma de solicitação do nome do usuário e uma senha. A autenticação resulta em um relacionamento confiável entre o cliente e o servidor, uma vez que o servidor confie no cliente, ele concederá ou negará acesso a determinados recursos.

Nestes termos, o controle de acesso à intranet no TRT é restrito aos usuários da organização, ou seja, só quem tem usuário/senha é liberado para acessá-la. Este procedimento, por sua vez, se distingue do acesso à rede de informática (como o fornecimento do usuário/senha para utilização do computador da organização). Cada serviço da intranet torna-se individualizado, além disso diferentes serviços são acessados e empregam diferentes acessos usuários/senhas.

Portanto, este dispositivo de segurança utilizado no TRT é abordado por Evans (1998), cujo acesso a servidores, páginas individuais ou diretórios inteiros da *web* são feitos mediante um nome de usuário e senha. O TRT utiliza-se de *software* de *password* para todos os programas da intranet, vale destacar que se pretende implantar um sistema de identidade única, ou seja, uma vez identificado usuário e senha, ele terá acesso a tudo

que é permitido com esta única identidade. A implantação de um sistema de segurança no TRT surge a partir de um problema detectado. O Tribunal era comumente alvo de ataques proporcionado por sua abertura à rede Internet, era constantemente atacada por vírus e *spams*. As providências adotadas foram a utilização de mecanismos de proteção como antivírus na entrada da rede, junto ao *firewall*, aperfeiçoaram os sistemas de proteção contra vírus nas próprias estações.

Quanto ao controle da área externa (Internet), o acesso de clientes externos à rede do TRT, faz-se através de *gateways* ou *firewalls*. Já o acesso interno para o externo o Tribunal dispõe do DMZ (ver figura 1 em apêndice B). O DMZ é uma área de rede separada logicamente e também fisicamente, onde ficam instalados os servidores de rede, banco de dados e todas as informações e sistemas do Tribunal. O usuário para ter acesso a esta área tem que dispor de permissão e senha, através de *gateway* e *firewall*.

Um *firewall*, segundo O'brien (2004), atua como um sistema de computador guardião, que protege as intranets e outras redes de computadores da empresa contra a invasão, funcionando como um filtro e é considerado ponto seguro de transferência para acesso à Internet e outras redes. No TRT é capaz de filtrar todo o tráfego de rede em busca de senhas corretas ou outros códigos de segurança e permite transmissões autorizadas para dentro e para fora da rede. Com a reestruturação da rede de informática do TRT foi possível a interligação dos servidores utilizando *gateways* e *firewalls*, recursos que confirmam o principal objetivo, argumentado por Evans (1998), garantir a integridade e a segurança das informações. O acesso à página do TRT se faz fundamentalmente pelo uso de usuário/senha.

É importante salientar que o TRT dispõe do DMZ (divisão da rede), responsável pela criação de um grupo de servidores de rede que registra os caminhos que o usuário percorre enquanto lhe é solicitado a digitação do usuário/senha pela *gateway* de acesso.

As novas estruturações do Tribunal Regional do Trabalho advém com alterações tanto com relação à segurança física quanto lógica, confirmado pela existência de *firewalls* de antivírus, *firewalls* de *spam*, ou seja, *firewalls* específicos para extinguir os principais transtornos na rede. A reestruturação total, segundo Sandro Beltrame, sedimenta toda a

rede de informática por distribuição física, onde o primeiro e quarto andares do prédio estão isolados fisicamente juntamente com os servidores.

No entanto, de acordo com Stewart (1997), os *firewalls* atuam como bloqueios com a finalidade de impedir a entrada de algo indesejado, mas sua proteção nem sempre é possível quando *hackers* (invasores de sistemas) atravessam a Internet. Neste sentido, o Tribunal Regional do Trabalho já foi alvo de muitos ataques e seguindo a classificação de Soares, Lemos e Colcher (1995), já foi alvo do ataque personificado, cuja idoneidade foi mascarada em listas de *spam* e propagação de vírus difundidas pela ação de *hackers*.

Os *firewalls* são classificados, de acordo com Soares, Lemos e Colcher (1995) em três categorias principais: filtros de pacotes, *gateways* de circuito e *gateways* de aplicação.

Ainda, com relação aos filtros de pacotes, considerando a descrição dos autores anteriormente citados, no TRT é de responsabilidade do administrador que se encarrega pela elaboração de uma lista de máquinas e serviços que estão autorizados a transmitir datagramas nos possíveis sentidos de transmissão (entrada na rede interna, saindo na rede interna ou ambos), que é então usada para filtrar os datagramas ip que tentam atravessar o *firewall*. Já, os *gateways* de circuitos atuam como intermediários de conexões tcp, funcionando como um *proxy* tcp (um tcp modificado). Nesse sentido, de acordo com George Alexandre Silva – Assistente-Chefe do Setor de Administração de Sistemas Operacionais (SESOP) verifica-se a utilização pelo TRT do *firewall* atuante em conjunto com a tecnologia *gateway* ao filtro de pacotes. No mais, pode-se acrescentar quanto ao sistema operacional a presença do roteamento nativo do *linux* acrescido de *iptables*.

Os produtos *firewalls*, de acordo com Benett (1997), podem prestar muitos serviços Internet, inclusive http, ftp, dns e smtp (correio eletrônico), cada serviço oferecido dessa forma é chamado *proxy*. Ainda, segundo o autor, o programa *proxy* reside no *firewall* e tem acesso aos dois lados da interface – a intranet e a Internet.

As solicitações de serviços externos feitas a partir da empresa, como em um navegador *web* que aponte para um url remoto, são capturadas pelo *proxy* de serviço http e, se as normas do *firewall* permitirem, são transmitidas para a Internet.

Desta forma, os serviços no TRT estão basicamente divididos, segundo George Silva em:

a) serviços de arquivo com acesso através de usuário/senha;

b) servidor *web/nt* envolvendo:

- acesso *proxy* (externo);
- acesso intranet (*web*);
- acesso ftp;
- correio eletrônico;

c) aplicações internas acessados por usuário/senha tais como:

- sistemas de acompanhamento de processos de 1° e 2° graus (Sap I e Sap II);
- sistema único de protocolo (sup);
- sistema de pagamento.

Portanto, o tráfego na Internet dentro da organização é capturado pelo *proxy* de serviço e se as normas do *firewall* permitirem, é transmitido para utilização dos serviços disponibilizados na intranet do TRT/SC.

A utilização de *backups* também integra uma das práticas no que tange aos aspectos da segurança. Os *backups* são programas automatizados, ou seja, uma vez programados são capazes de desenvolver toda a rotina de *backup* automaticamente. Sua realização deve ser feita regularmente, de acordo com Stewart (1997), é uma maneira de garantir que os dados sejam protegidos.

Diante do exposto, a rotina de *backups* executadas no TRT é diária, semanal e mensal dependendo do critério estabelecido pela área de informática. O Diretor da Área de Suporte aos Recursos de Informática, Sandro Beltrame, comenta que são imprescindíveis para armazenar históricos de posições e não somente pelo aspecto da integridade, cujo *backup* diário já seria suficiente.

Em contrapartida, os *backups* podem tornar-se inúteis caso não forem atualizados e armazenados em local seguro. Segundo Stewart (1997), é interessante transportar regularmente os discos de *backups* para uma instalação de armazenamento em local diferenciado. Por isso, a prática do TRT é armazenar os *backups* em dois lugares distintos,

um deles é num cofre corta fogo, em uma sala diferente dos servidores de rede e o outro é restrito somente para os técnicos de informática.

Já quanto à segurança e proteção das informações constantes nos servidores de rede, o TRT mantém uma sala fechada contendo detectores de fumaça, sistema de combate à incêndio, alarmes de temperatura, alarmes de umidade, portanto, de restrição quanto ao acesso físico de qualquer colaborador da área de informática, tendo neste caso livre acesso à sala dos servidores de rede.

Assim, do ponto de vista das organizações deve-se reconhecer que a informação é um ativo de importância fundamental para a continuidade de suas atividades. A segurança de informações dentro de uma organização deve ser conscientizada pela aplicação de uma política geral de segurança baseada no valor intrínseco das informações que estão sendo protegidas. O TRT não foge à regra e define, para a sua intranet, políticas de segurança bem específicas, como se observa em seguida.

4.3 Verificação das políticas de segurança em informática adotadas

Uma política de segurança constitui um conjunto de regras, leis e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos. Neste sentido, as políticas de segurança no Tribunal são definidas pela área de informática, sendo consideradas principais as listadas a seguir:

a) acesso usuário/senha

b) restrição ao acesso

c) restrição ao uso

Segundo Soares, Lemos Colcher e (1995), um determinado sistema é considerado seguro em relação a uma política de segurança, caso garanta o cumprimento das leis, regras e práticas definidas nessa política.

Conforme o exposto, pode-se considerar seguros os sistemas implantados pelo TRT tendo em vista que seus principais itens são atendidos. Os itens principais definidos e em

conformidade com a política de segurança adotada pelo TRT/SC para atender a segurança administrativa são: segurança física, controle de integridade (como *backups*), controle de acesso.

Uma política de segurança inclui regras determinando como as informações e recursos devem ser manipulados no contexto organizacional. Desta forma, o TRT registra no sistema a negação ao ambiente externo (Internet), bem como, controla *sites* acessados por cada colaborador responsabilizando-os pelo descumprimento ao acesso de *sites* não autorizados. Sobre este aspecto da segurança Starlin e Novo (1998) afirmam que a garantia da segurança é considerada um dos processos básicos e prioritários para usuários de uma rede corporativa e para os sistemas e aplicativos utilizados através desta.

Atualmente o TRT apresenta, de forma geral, resistências quanto às política de segurança, pelo fato de restringir acessos sob novas condições e pelo monitoramento de ações que antes não eram consideradas utilizando-se *gateways* e *firewalls* para permitir o acesso aos servidores.

Nestes termos, Stewart (1997) confirma o mecanismo utilizado pelo TRT tendo em vista que não é só possível que uma empresa monitore a atividade do colaborador por meio de uma intranet, como também é considerado legal. A política de segurança também inclui monitoramento contra acessos indevidos e eventuais riscos aos sistemas que asseguram suas informações.

4.4 Levantamento dos mecanismos utilizados pelo TRT para redução do nível de resistência e conscientização dos usuários quanto à segurança

A evolução da tecnologia, principalmente no que se refere aos recursos computacionais, vem estabelecendo de forma generalizada uma nova concepção em termos de necessidades a serem atendidas. A partir desta análise pode-se afirmar que a implantação de um novo sistema de segurança no TRT surge no momento que a organização detecta um problema na forma de vírus, *spams* ou *hackers*. Primeiramente,

verifica-se o problema, a partir daí um diagnóstico é traçado e finalmente identifica-se a possibilidade de falhas no sistema que podem ser causadas por erros no *software, hardware*, atraso no sistema ou até mesmo erro humano (manipulação de dados, inclusão de dados). A verificação depende de um sistema para outro sendo que cada qual utiliza-se de uma metodologia específica.

Desse modo, o TRT vem se adequando à capacidade de integração de tecnologias conduzindo a novos modelos de gerenciamento como a reestruturação de sua rede de informática com a interligação dos servidores utilizando *gateways* e *firewalls* e pela implantação de um sistema de identidade única provocando mudanças. Quanto a este aspecto, Rodrigues e Ferrante (1995) consideram que as principais mudanças dentro das organizações são do tipo cultural e comportamental. Neste sentido, a implantação de novos sistemas no TRT desencadeia muita resistência, por isso a organização empenha-se na realização de programas intensivos de treinamento, palestras e colaboração dos usuários da rede.

Ao elaborar um sistema, a área de informática do TRT convoca os usuários da rede com o objetivo de atenuar a resistência e a rejeição ao sistema, pois a aceitação e adaptação à mudança é facilitada quando os próprios usuários participam.

Desta forma, pode-se constatar que o Tribunal Regional do Trabalho, ao fazer programas de treinamento, está diante da solução mais efetiva, segundo Stewart (1997), de gerenciamento de pessoas que utilizam a intranet. A intranet está dirigida às pessoas que trabalham na organização, o público-alvo que utiliza seus serviços, de acordo com Stewart (1997) é formado por usuários que detém algum tipo de acesso à intranet.

Neste contexto, a implantação de sistemas de segurança, sendo um recurso de inovação tecnológica e mudança organizacional, afetam o ambiente dos usuários de rede. Considerando o Tribunal Regional do Trabalho, cabe destacar que as maiores dificuldades na implantação de um sistema de segurança faz-se pela resistência às mudanças e pelo incremento de burocracias que costumeiramente afetam as rotinas de trabalho.

5 CONSIDERAÇÕES FINAIS

Sabe-se que atualmente as organizações lidam com uma gama surpreendente de informações capazes de alterar o ambiente organizacional provocando mudanças de comportamento diante da nova realidade. A partir da necessidade em armazenar e capturar informações consideradas valiosas, as organizações vêm adquirindo dependências em termos de uso da tecnologia de informações em maior ou menor grau. O grau de dependência agravou-se muito em função da tecnologia de informática, que permite reunir grande quantidade de informações em seus sistemas.

No entanto, a facilidade em conter as informações envolve aspectos relacionados ao risco de violações desses recursos tecnológicos. Na realidade, quando há implementação de segurança em ambiente de informações, procura-se eliminar, o máximo possível pontos fracos ou garantir o máximo de segurança para a organização. O meio de registro torna-se concomitantemente, meio de armazenamento, acesso e divulgação.

Neste contexto, insere-se a realidade do Tribunal Regional do Trabalho de Santa Catarina, empresa do setor público, que tem demonstrado utilizar-se de recursos tecnológicos no que se refere aos sistemas de segurança tanto física quanto lógica na sua rede interna – intranet.

A intranet no Tribunal é de uso restrito e seu acesso é liberado quando há autenticação do usuário e senha. Cada serviço da intranet torna-se individualizado e seu controle quanto à navegação é basicamente realizado pelos *gateways* e *firewalls* implantados na rede.

Um fato interessante que cabe destacar quanto à autenticação por meio do sistema usuário e senha no TRT refere-se a responsabilidade pela alteração da mesma. Ou seja, ao usuário não é exigido através de sistemas, a troca periódica e obrigatória das senhas. Pode-se constatar a partir do embasamento teórico deste trabalho, que este fato implica numa ameaça ao sistema, tendo em vista que as informações não podem se manter confidenciais indefinidamente.

Já com relação à segurança física, pôde-se constatar que o TRT dispõe de um sofisticado sistema de proteção dos servidores de rede em salas climatizadas compostas por detectores de fumaça, ar-condicionado central, sistema de combate a incêndio e alarmes que controlam a temperatura local e a umidade.

A implementação da segurança constitui fator imprescindível num ambiente em que predominam informações de caráter público. É importante ressaltar que muitas organizações não sobrevivem por longo tempo frente a um colapso do fluxo de informações, não importando qual o meio de armazenamento adotado. E, dada a característica de uma organização de grande porte como é o caso do TRT, um colapso no fluxo de informações acarreta num enorme transtorno quanto ao controle e administração gerencial.

Em virtude desta eventual situação, o TRT implanta uma estrutura de segurança promitente, pelo fato de já ter sido alvo de invasões e ataques nos sistemas de rede. Assim, as diretrizes e a definição de políticas de segurança são de responsabilidade da área de informática, suas atribuições procuram ser repassadas a todos os colaboradores de modo a conscientizá-los da importância do seu envolvimento direto quanto à integridade e eficácia dos sistemas de informações na rede.

Desta forma, a realidade organizacional em termos de segurança no Tribunal Regional do Trabalho mostra-se atenta às ameaças, invasões e quaisquer outras formas de violação à integridade das informações tanto na rede interna (intranet) quanto na externa (Internet).

REFERÊNCIAS

ALBERTIN, Alberto Luiz. **Comércio eletrônico**: um modelo, aspectos e contribuições de sua aplicação. 2.ed. São Paulo: Atlas, 2000.

ANTHONY, Robert. **Sistemas de controle gerencial.** São Paulo: Atlas, 2001.

BABBIE Eal. **The practice of social research.** California: wadsworth publishing company, 1998.

BARAN, Nicholas. **Desvendando a superestrada da informação.** Rio de Janeiro: Campus, 1995.

BENNETT,Geoff. **Internetworking com tcp/ip:** protocolos, services, segurança e performance.Rio de Janeiro: Infobook,1998.

BENNETT, Gordon. **Intranets:**como implantar com sucesso na sua empresa.Rio de Janeiro: Campus,1997.

CARLOS, Alberto Júlio; SALIBI NETO, José. **Inovação e mudança:** autores e conceitos imprescindíveis. São Paulo: Publifolha, 2001.

CARUSO, Carlos A.A. **Segurança em informática e de informações.** São Paulo: Senac, 1999.

CASSARRO, Antônio Carlos. **Controles internos e segurança de sistemas**: prevenindo fraudes e tornando auditáveis os sistemas. São Paulo: Ltr,1997.

CHIAVENATO, Idalberto. **Introdução à teoria geral da administração**: uma visão abrangente da moderna administração das organizações. 7.ed. Rio de Janeiro: Elsevier, 2003.

CRUMLISH, Christian. **Explorando a internet.** São Paulo: Makron books, 1995.

DAY, George S. **A empresa orientada para o mercado:** compreender, atrair e manter clientes valiosos. Porto Alegre: Bookman, 2001.

EVANS, Tim. **Construindo uma intranet**.São Paulo: Makron books, 1998.

FANTINATTI, João Marcos. **Segurança em informática**: metodologia e prática. São Paulo: Mcgraw-hill, 1988.

GAITHER,Mark, HASSINGER Sebastian,ERWIN Mike. **World wide *web* com *html* & cgi**: bíblia do programador. São Paulo:Berkeley Brasil,1996.

GIL, Antônio de Loureiro.**Segurança em informática.** São Paulo: Atlas, 1994.

JACOBSEN, Alessandra Linhares. Implicações do uso da tecnologia de informação como recurso de inovação no ambiente organizacional. **Revista ciências da administração.** Florianópolis, v.2 , nº4, p.07-09, set.2000.

MATTAR, Fauze Najib. **Pesquisa de marketing**. 3.ed. São Paulo: Atlas, 2001.

_____. **Pesquisa de marketing** : metodologia, planejamento.5 .ed. São Paulo: Atlas, 1999.

MELO, Ivo Soares. **Administração de sistemas de informação**. São Paulo: Pioneira, 1999.

MONTANA, Patrick J, CHARNOV Bruce H. Administração. São Paulo: Saraiva, 1999.

O'BRIEN, James A. **Sistemas de informação e as decisões gerenciais na era da Internet**. 2.ed. São Paulo: Saraiva, 2004.

RODRIGUEZ, Martius V; FERRANTE, Augustin J. **A Tecnologia de informação e mudança organizacional**. Rio de Janeiro: Infobook, 1995.

SOARES, Luiz Fernando G.LEMOS, Guido e COLCHER, Sérgio. **Redes de computadores**: das lans, mans e wans às redes atm. Rio de Janeiro: Campus, 1995.

STARLIN, Gorki, NOVO Rafael. **Segurança na Internet**: um guia de tecnologia e produtos contra os hackers. Rio de Janeiro Book Express ltda, 1998.

STEWART, James M. **Intranet bíblia.** São Paulo: Berkeley Brasil, 1997.

TAIT, Tânia Fátima Calvi. **Um modelo de arquitetura de sistemas de informação para o setor público:** um estudo em empresas estatais prestadoras de serviços de informática. 2000. 242f. Tese (Doutorado) – Programa de Pós-Graduação Engenharia da Produção, Universidade Federal de Santa Catarina, Florianópolis, 2000.

TANENBAUM, Andrew S. **Redes de computadores**. Rio de Janeiro: Campus, 1994.

TRIBUNAL Regional do Trabalho. Disponível em: http://www.trt12.gov.br/. Acessado em 07 de maio de 2005.

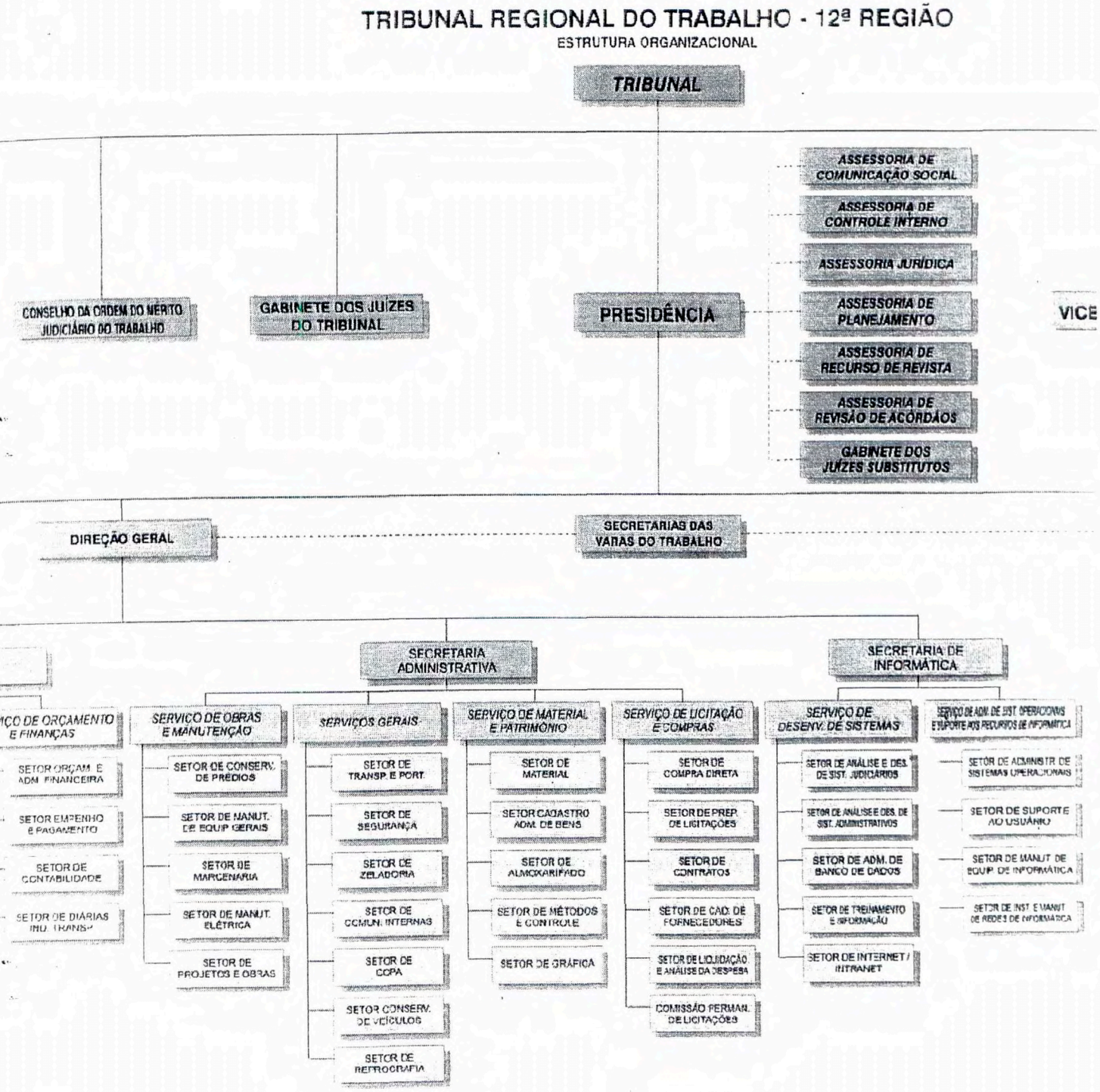
VERGARA, Silvia C. **Projetos e relatórios de pesquisa em administração.** São Paulo: Atlas, 1997.

VOLPI, Marlon Marcelo. **Assinatura digital**: aspectos técnicos, práticos e legais.Rio de Janeiro: Axcel Books do Brasil, 2001.

WEINMAN, William E. **Manual de cgi.** São Paulo: Makron books, 1997.

WOOD JR., Tomaz . **Mudança organizacional**. 3.ed. São Paulo: Atlas, 2002.

ANEXO A


TRIBUNAL REGIONAL DO TRABALHO - 12ª REGIÃO
ESTRUTURA ORGANIZACIONAL
TRIBUNAL
CONSELHO DA ORDEM DO MERITO JUDICIÁRIO DO TRABALHO
GABINETE DOS JUIZES DO TRIBUNAL
PRESIDÊNCIA
ASSESSORIA DE COMUNICAÇÃO SOCIAL
ASSESSORIA DE CONTROLE INTERNO
ASSESSORIA JURÍDICA
ASSESSORIA DE PLANEJAMENTO
ASSESSORIA DE RECURSO DE REVISTA
ASSESSORIA DE REVISÃO DE ACÓRDÃOS
GABINETE DOS JUIZES SUBSTITUTOS
VICE
DIREÇÃO GERAL
SECRETARIAS DAS VARAS DO TRABALHO
SECRETARIA ADMINISTRATIVA
SECRETARIA DE INFORMÁTICA
ÇO DE ORÇAMENTO E FINANÇAS
SETOR ORÇAM. E ADM. FINANCEIRA
SETOR EMPENHO E PAGAMENTO
SETOR DE CONTABILIDADE
SETOR DE DIÁRIAS INDJ. TRANSP.
SERVIÇO DE OBRAS E MANUTENÇÃO
SETOR DE CONSERV. DE PRÉDIOS
SETOR DE MANUT. DE EQUIP. GERAIS
SETOR DE MARCENARIA
SETOR DE MANUT. ELÉTRICA
SETOR DE PROJETOS E OBRAS
SERVIÇOS GERAIS
SETOR DE TRANSP. E PORT.
SETOR DE SEGURANÇA
SETOR DE ZELADORIA
SETOR DE COMUN. INTERNAS
SETOR DE COPA
SETOR CONSERV. DE VEÍCULOS
SETOR DE REPROGRAFIA
SERVIÇO DE MATERIAL E PATRIMÔNIO
SETOR DE MATERIAL
SETOR CADASTRO ADM. DE BENS
SETOR DE ALMOXARIFADO
SETOR DE MÉTODOS E CONTROLE
SETOR DE GRÁFICA
SERVIÇO DE LICITAÇÃO E COMPRAS
SETOR DE COMPRA DIRETA
SETOR DE PREP. DE LICITAÇÕES
SETOR DE CONTRATOS
SETOR DE CAD. DE FORNECEDORES
SETOR DE LIQUIDAÇÃO E ANÁLISE DA DESPESA
COMISSÃO PERMAN. DE LICITAÇÕES
SERVIÇO DE DESENV. DE SISTEMAS
SETOR DE ANÁLISE E DES. DE SIST. JUDICIÁRIOS
SETOR DE ANÁLISE E DES. DE SIST. ADMINISTRATIVOS
SETOR DE ADM. DE BANCO DE DADOS
SETOR DE TREINAMENTO E INFORMAÇÃO
SETOR DE INTERNET / INTRANET
SERVIÇO DE ADM. DE SIST. OPERACIONAIS E SUPORTE AOS RECURSOS DE INFORMÁTICA
SETOR DE ADMINISTR. DE SISTEMAS OPERACIONAIS
SETOR DE SUPORTE AO USUÁRIO
SETOR DE MANUT. DE EQUIP. DE INFORMÁTICA
SETOR DE INST. E MANUT. DE REDES DE INFORMÁTICA

TRT 12ª Região - Usuário: Sandro Beltrame - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

http://intranet.trt12.gov.br/intranet/intranet_index.asp

HOME TRT

intranet

SERVIÇOS

ÁREAS DO TRT

SERVIÇOS
Alteração de senha - correio
Boletim de Serviço
Cálculos Trabalhistas
Catálogo Telefônico
Chamada SAJUD
Chamada SUPORTE
Comissão SAP 1
Consulta a Processos - 1º Grau
Consulta a Processos - 2º Grau
Consulta Bens da Unidade

INFORMAÇÕES

:: SUP-Sistema Único de Protocolo
:: SUP : Manual e informações diversas
:: Manual sistema FGTS (.doc)
:: Varas Trabalhistas no Brasil
:: Trâmite Processual de 2º Grau
:: Projeto de Intimação Judicial

recionamento

es.

SUP Sistema Único de Protocolo

Estrutura Funcional

Consulte o seu Contracheque

Alteração da senha

Organograma do TRT (.pdf)

CEP | AJUT | SINTRAJUSC | OAB-SC

Convênios

Bacenjud

Depósitos Judiciais para Magistrados

CAIXA FGTS Depósitos Recursais

DETRAN/SC

Dúvidas ou sugestões?

Fale conosco !

ANEXO-B

Erro na página.

APÊNDICE A

ROTEIRO PARA A ENTREVISTA

1) O que é informação e porque ela é importante?
2) Quem é responsável pelos dados da organização?
3) Quais os serviços da rede que podem ser acessados pela organização, esse acesso é restrito (dentro da internet)?
4) Qual o nível de importância da tecnologia na empresa?
5) Quais mecanismos de segurança são usados para controlar o acesso à rede?
6) Qual a tecnologia usada na intranet (tcp/ip)? Quem desenvolve?
7) Quais as providências tomadas para proporcionar o mínimo de proteção e integridade das informações?
8) Quais são as preocupações básicas que constituem o enfoque da segurança?
9) Quais são as seguranças físicas e lógicas existentes?
10) O que você entende por Sistema de segurança?
11) A implantação de um sistema de segurança é simples?
12) Quais as maiores dificuldades na implantação de um sistema de segurança?
13) A implantação de novos sistemas é percebida de modo aceitável? Há muita resistência por parte dos colaboradores?
14) Qual a periodicidade na implantação de um sistema de segurança e quando a empresa vê a necessidade de implantar novos sistemas?
15) Qual é o principal critério que deve nortear o direito de acesso à determinada informação?
16) Quais as medidas de proteção relacionadas com o controle de acesso
17) Você considera que há controles rigorosos em relação ao acessos lógicos? Há muitas restrições no acesso às informações?
18) A substituição de senhas é um procedimento aleatório e frequente?
19) Existe software de password?
20) Quais os principais tipos de arquivos que devem ter cópias de segurança?
21) Há programas que procedam a geração automática de backups? Quando este é feito (periodicidade/horário)?
22) Vocês utilizam sistema de programação para usuários relacionado à segurança como o Lotus Notes?
23) Existe uma política de segurança na organização?
24) Quais são os principais itens que devem ser verificados em uma política de segurança para atender à segurança administrativa?
25) Qual a importância da cultura da organização para uma política de segurança?
26) A política de segurança sofre resistências dentro da organização?

27) Como é feita a conscientização das pessoas com relação à segurança (Treinamentos, Palestras, folders)?
28) Quais são as principais ameaças à rede na sua opinião (vírus, cavalo de tróia, worms)?
29) Quais são os fatores que influenciam a falta de segurança nas redes?
30) Quanto a segurança física, o ambiente de informações está bem aparelhado em termos de equipamentos de prevenção e extinção de incêndio?
31) Quais foram os problemas a serem sanados por descuidos na segurança física e lógica?
32) Quais são os software de proteção (aplicativo, básico), como funcionam?
33) Quem tem acesso à intranet? Que aplicativos são limitados e porquê?
34) Quais os mecanismos de segurança da intranet?
35) Quais são as vantagens e desvantagens de uma intranet?
36) Qual é a infra-estrutura básica de hardware e software necessária para implementar a intranet?
37) Quais áreas de dados são públicas, restritas ou disponíveis às pessoas ?
38) Como funcionam e em quais locais do sistema estão as gateways que controlam o acesso aos dados e as rotinas de manipulação?
39) Como distinguir um problema real de software ou hardware de um erro humano ou atraso no sistema?
40) Qual a tecnologia utilizada para o correio eletrônico?
41) Quais os principais problemas de segurança relacionados ao correio eletrônico?
42) Quais são as fontes de informação e serviço que a intranet oferece (lista de pesquisa, mapas)?
43) Quais são as fontes de recursos disponibilizadas numa intranet (help desk, documentos existentes em processadores de textos, planilhas e outros aplicativos compartilhados)?

APÊNDICE B

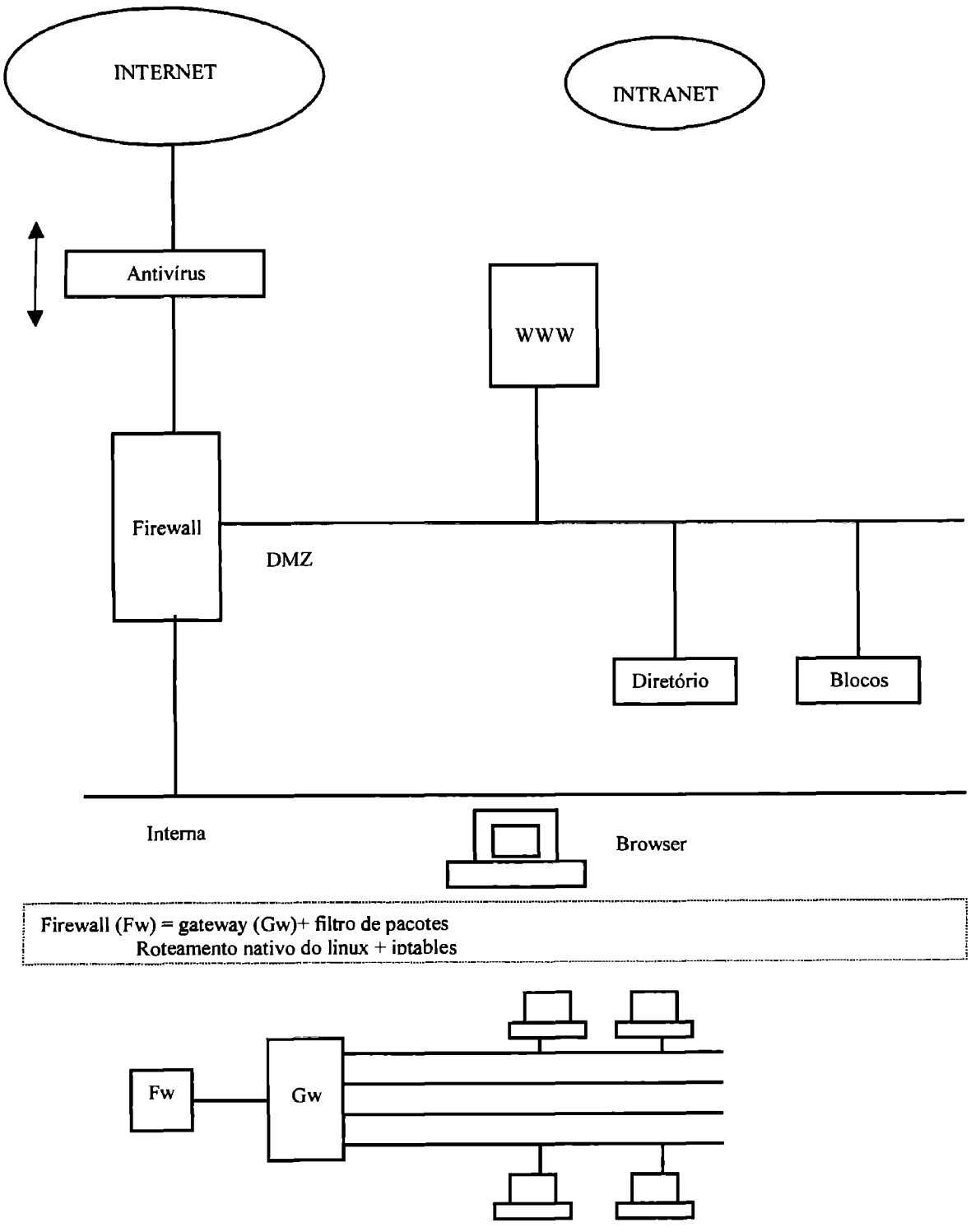


Figura 1: esquema de segurança na intranet – TRT/SC. Fonte: dados primários, 2005